IJCSIS Vol. 10 No. 12, December 2012
ISSN 1947-5500

International Journal of Computer Science & Information Security


Cornell University
Library


Cogprints


Google scholar


.docstoc
find and share professional documents


ScientificCommons

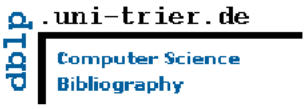

View my documents on
Scribd


BASE
Bielefeld Academic Search Engine


SCIRUS
search engine for science


SciRate.com


CiteSeerx beta


dblp .uni-trier.de
Computer Science
Bibliography


Q·Sensei


DOAJ
DIRECTORY OF
OPEN ACCESS
JOURNALS


EBSCO
HOST


ProQuest

Editorial
Message from Managing Editor

*Since May 2009, the **International Journal of Computer Science and Information Security** (IJCSIS), promotes dissemination of knowledge in research areas of computer applications and practices, and advances in information security. The research themes focus mainly on innovative developments, research issues/solutions in computer science and related technologies.*

IJCSIS archives publications, abstracting/indexing, editorial board and other important information are available online on homepage. IJCSIS editorial board consisting of reputable experts solicits your research contribution to the journal with your research papers, projects, surveying works and industrial experiences. IJCSIS appreciates all the insights and advice from authors and reviewers. Indexed by the following International Agencies and institutions: Google Scholar, Bielefeld Academic Search Engine (BASE), CiteSeerX, SCIRUS, Cornell's University Library EI, Scopus, DBLP, DOI, ProQuest, EBSCO. Google Scholar reported a large amount of cited papers published in IJCSIS.

IJCSIS is currently accepting manuscripts for upcoming issues based on original qualitative or quantitative research, an innovative conceptual framework, or a substantial literature review that opens new areas of inquiry and investigation in Computer science. Case studies and works of literary analysis are also welcome.

*We look forward to your collaboration. For further questions please do not hesitate to contact us at **ijcsiseditor@gmail.com**.*

A complete list of journals can be found at:
http://sites.google.com/site/ijcsis/

IJCSIS Vol. 10, No. 12, December 2012 Edition

ISSN 1947-5500 © IJCSIS, USA.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

IJCSIS

ISSN (online): 1947-5500

Please consider to contribute to and/or forward to the appropriate groups the following opportunity to submit and publish original scientific results.

CALL FOR PAPERS
International Journal of Computer Science and Information Security (IJCSIS)
January-December 2013 Issues

The topics suggested by this issue can be discussed in term of concepts, surveys, state of the art, research, standards, implementations, running experiments, applications, and industrial case studies. Authors are invited to submit complete unpublished papers, which are not under review in any other conference or journal in the following, but not limited to, topic areas.
See authors guide for manuscript preparation and submission guidelines.

Indexed by Google Scholar, DBLP, CiteSeerX, Directory for Open Access Journal (DOAJ), Bielefeld Academic Search Engine (BASE), SCIRUS, Cornell University Library, ScientificCommons, EBSCO, ProQuest and more.

Deadline: see web site
Notification: see web site
Revision: see web site
Publication: see web site

Context-aware systems
Networking technologies
Security in network, systems, and applications
Evolutionary computation
Industrial systems
Evolutionary computation
Autonomic and autonomous systems
Bio-technologies
Knowledge data systems
Mobile and distance education
Intelligent techniques, logics and systems
Knowledge processing
Information technologies
Internet and web technologies
Digital information processing
Cognitive science and knowledge
Agent-based systems
Mobility and multimedia systems
Systems performance
Networking and telecommunications
Software development and deployment
Knowledge virtualization
Systems and networks on the chip
Knowledge for global defense
Information Systems [IS]
IPv6 Today - Technology and deployment
Modeling
Software Engineering
Optimization
Complexity
Natural Language Processing
Speech Synthesis
Data Mining

For more topics, please see web site https://sites.google.com/site/ijcsis/

For more information, please visit the journal website (https://sites.google.com/site/ijcsis/)

TABLE OF CONTENTS

8. Paper 30111233: A Discrete Event Simulation Approach on Polarized based Quantum Key Distribution Protocols using OptiSystem™ (pp. 42-48)

Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K.Subramaniam
FSKTM, University Putra Malaysia, Serdang, Malaysia
Hishamuddin Zainuddin, INSPEM, University Putra Malaysia, Serdang, Malaysia
Suhairi Saharudin, MIMOS BERHAD, Technology Park Malaysia, KL, Malaysia

Enhancing the retrieval performance by combing the texture and edge features

Mohamed Eisa
Computer Science Department
PortSaid University

Amira Eletrebi
Computer Science Department
Mansoura University

Ebrahim Elhenawy
Computer Science Department
Zagazig University

Abstract— **In this paper, anew algorithm which is based on geometrical moments and local binary patterns (LBP) for content based image retrieval (CBIR) is proposed. In geometrical moments, each vector is compared with the all other vectors for edge map generation. The same concept is utilized at LBP calculation which is generating nine LBP patterns from a given 3x3 pattern. Finally, nine LBP histograms are calculated which are used as a feature vector for image retrieval. Moments are important features used in recognition of different types of images. Two experiments have been carried out for proving the worth of our algorithm. The results after being investigated shows a significant improvement in terms of their evaluation measures as compared to LBP and other existing transform domain techniques.**

Keywords- CBIR; Feature extraction; geometrical moments; Local Binary Patterns.

I. INTRODUCTION

With the rapid expansion of worldwide network and advances in information technology there is an explosive growth of multimedia databases and digital libraries. This demands an effective tool that allow users to search and browse efficiently through such a large collections [1].

In many areas of commerce, government, academia, hospitals, entertainment, and crime preventions large collections of digital images are being created. Usually, the only way of searching these collections was by using keyword indexing, or simply by browsing. However, as the databases grew larger, people realized that the traditional keywords based methods to retrieve a particular image in such a large collection are inefficient. To describe the images with keywords with a satisfying degree of concreteness and detail, we need a very large and sophisticated keyword system containing typically several hundreds of different keywords. One of the serious drawbacks of this approach is the need of trained personnel not only to attach keywords to each image (which may take several minutes for one single image) but also to retrieve images by selecting keywords, as we usually need to know all keywords to choose good ones. Further, such a keyword based approach is mostly influenced by subjective decision about image content and also it is very difficult to change a keyword based system afterwards. Therefore, new techniques are needed to overcome these limitations [2].

Digital image databases however, open the way to content based searching. It is common phrase that an image speaks thousands of words. So instead of manual annotation by text based keywords, images should be indexed by their own visual contents, such as color, texture and shape. [3]The main advantage of this method is its ability to support the visual queries. Hence researchers turned attention to content based image retrieval (CBIR) methods.

Several methods achieving effective feature extraction have been proposed in the literature [4].

[5] Introduced the histogram intersection distance metric to measure the distance between the histograms of images. Stricker et al [6] used the first three central moments called mean, standard deviation and skewness of each color for image retrieval. Pass et al. introduced color coherence vector (CCV) [7].

The recently proposed local binary pattern (LBP) features are designed for texture description. The recently,[8], proposed the LBP and these LBPs are converted to rotational invariant for texture classification. we proposed the rotational invariant texture classification using feature distributions. [9] used the LBP operator facial expression analysis and recognition. Heikkila et al. proposed the background modeling and detection by using LBP. Huang et al. proposed the extended LBP for shape localization. Heikkila et al. used the LBP for interest region description. Li et al. used the combination of Gabor filter and LBP for texture segmentation. Zhang et al. proposed the local derivative pattern for face recognition [10]. They have considered LBP as a nondirectional first order local pattern, which are the binary results of the first-order derivative in images.

II. GEOMETRICAL MOMENTS

The shape of an object is a very important character in human's perception, recognition, and comprehension. Because geometric shape represents the essential characteristic of an object, and has invariance with respect to translation, scale and orientation, the analysis and discernment like geometry are of important significance in computer vision. Historically, Hu published the first significant paper on the use of image moment invariants for two-dimensional pattern recognition applications [11]. His approach is based on the work of the 19th century mathematicians Boole, Cayley and Sylvester, and on the theory of algebraic forms.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$M_1 = \mu_{20} + \mu_{02} \quad (1)$$

$$M_2 = (\mu_{20} - \mu_{02})^2 + 4\mu_{11}^2 \quad (2)$$

$$M_3 = (\mu_{30} - 3\mu_{12})^2 + 3(\mu_{21} + \mu_{03})^2 \quad (3)$$

$$M_4 = (\mu_{30} + \mu_{12})^2 + (\mu_{21} + \mu_{03})^2 \quad (4)$$

$$M_5 = (\mu_{30} - 3\mu_{12})(\mu_{30} + \mu_{12})\left[(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2\right] + (3\mu_{21} - \mu_{03})(\mu_{21} + \mu_{03})\left[3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2\right] \quad (5)$$

$$M_6 = (\mu_{20} - \mu_{02})\left[(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2\right] + 4\mu_{11}(\mu_{30} + \mu_{12})(\mu_{21} + \mu_{03}) \quad (6)$$

$$M_7 = (3\mu_{21} - \mu_{03})(\mu_{30} + \mu_{21})\left[(\mu_{30} + \mu_{12})^2 - 3(\mu_{21} + \mu_{03})^2\right] + (3\mu_{12} - \mu_{30})(\mu_{21} + \mu_{03})\left[3(\mu_{30} + \mu_{12})^2 - (\mu_{21} + \mu_{03})^2\right] \quad (7)$$

Geometric moments of a $1D$ signal $S(x)$ are defined by [12]:

$$M_n(x) = \int_{-\omega}^{\omega} S(x+t)t^n dt \qquad n = 0,1,2,... \quad (8)$$

Where $M_n(x)$ is the moment of order n calculated from a window of size $(2\omega + 1)$ pixels centered at the point x. Geometric moments of a 2D image $I(x, y)$ are defined by [13]:

$$M_{mn}(x,y) = \int_{-\omega_1}^{\omega_1}\int_{-\omega_2}^{\omega_2} I(x+u, y+v)u^m v^n du dv \quad m,n = 0,1,2.. \quad (9)$$

Where $M_{m,n}(x)$ is the moment of order (m, n) calculated from a window of size $(2\omega_1 + 1) \times (2\omega_2 + 1)$ pixels centered at the pixel (x, y).

III. Local Binary Patterns

[14] proposed the local binary pattern (LBP) operator which describes the surroundings of a pixel by generating a bit-code from the binary derivatives of a pixel as a complementary measure for local image contrast. The LBP operator takes the eight neighboring pixels using the center gray value as a threshold. The operator generates a binary code 1 if the neighbor is greater or equal than the center otherwise generates a binary code 0. The eight neighboring binary code can be represented by a 8-bit number [15]. The LBP operator outputs for all the pixels in the image can be accumulated to form a histogram. Fig.1 shows an example of LBP operator. For given a center pixel in the image, LBP value is computed by comparing it with those of its neighborhoods:

$$LBP_{P,R} = \sum_{i=0}^{p-1} 2^i x f(g_i - g_c) \quad (10)$$

$$f(x) = \begin{cases} 1 & x \geq 0 \\ 0 & else \end{cases} \quad (11)$$

Where g_c is the gray value of the center pixel, g_i is the gray value of its neighbors, P is the number of neighbors and R is the radius of the neighborhood. Fig. 2 shows the examples of circular neighbor sets for different configurations of (P,R) .

The LBP measure the local structure by assigning unique identifiers, the binary number, to various microstructures in the image. Thus [16], LBP capture many structures in one unified framework. In the example in Fig. 3(b), the local structure is a vertical edge with a leftward intensity gradient. Other microstructures are assigned different LBP codes, e.g., corners and spots, as illustrated in Fig. 4. By varying the radius R and the number of samples P, the structures are measured at different scales, and LBP allows for measuring large scale structures without smoothing effects, as is, e.g., the case for Gaussian-based filters.

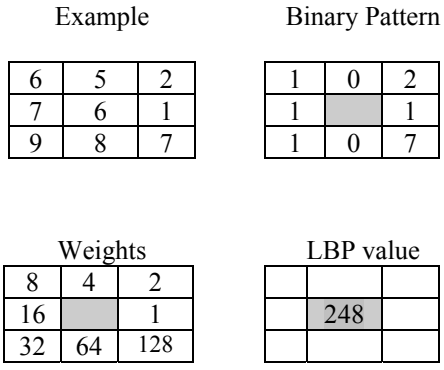


Fig. 1: LBP calculation for $3x3$ pattern

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

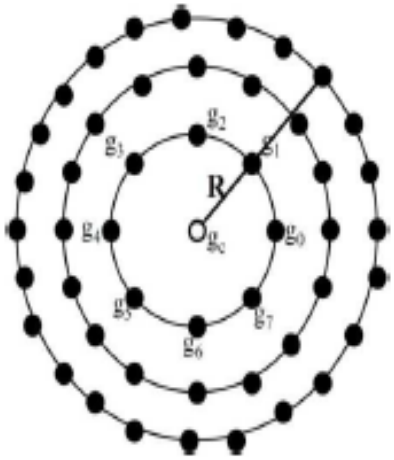


Fig. 2: Circular neighborhood sets for different (P,R)

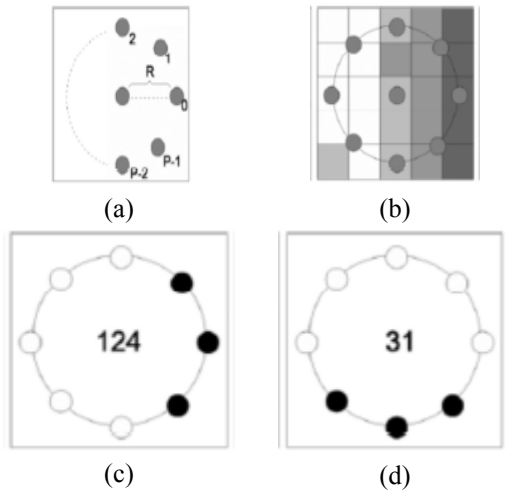


Fig. 3. Illustration of LBP. (a)The LBP filter is defined by two parameters; the circle radius R and the number of samples P on the circle. (b) Local structure is measured w. r. t. a given pixel by placing the center of the circle in the position of that pixel. (c) Samples on the circle are binarized by thresholding with the intensity in the center pixel as threshold value. Black is zero and white is one. The example image shown in (b) has an LBP code of 124. (d) Rotating the example image in (b) 900 clockwise reduces the LBP code to 31, which is the smallest possible code for this binary pattern. This principle is used to achieve rotation invariance.

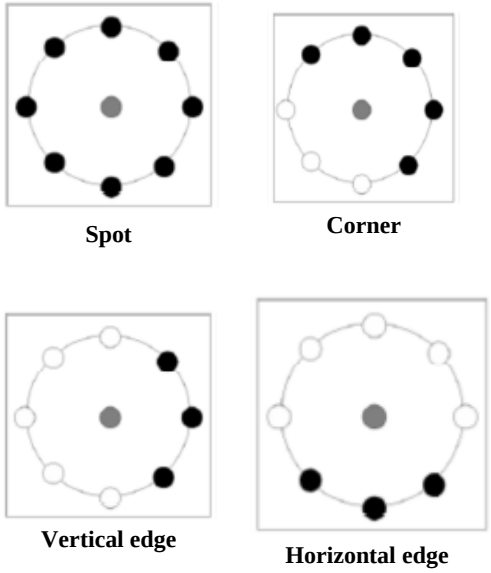


Fig 4: Various microstructures measured by LBP. The gray circle indicates the center pixel. Black and white circles are binarized samples; black is zero and white is one.

IV. FEATURES EXTRACTION

The weighted graph $(L_i\ X_i\ et\ al.,)$ with no self loops is $G = (V, E, W)$, where $V = \{1, 2, ..., N\}$ the node set is ($N = m.n$ is the total number of pixels in $Q \in R^{mxn}$) $E \subseteq VxV$ represents the edge set, and $W = (w_{ij})_{NxN}$ denotes an affinity matrix with the element w_{ij} being the edge weight between nodes i and j.

Based on the geometric moment's theory we compare the each pixel of $3x3$ pattern with remaining eight pixel gray values for generating binary code [17]. Finally, nine LBP patterns are collected for LBP histogram calculation and these are used as a feature vector for image retrieval [18].

A. Proposed System Framework (GMLBP)

Algorithm:

Input: Image; Output: Retrieval Result

1. Load the input image.
2. Collect the $3x3$ pattern for a center pixel i.
   - Construct the graph cut for $3x3$ pattern.
   - Generate nine LBP patterns.
   - Go to next center pixel.
3. Calculate the geometric moments LBP (GMLBP) histograms [19].
4. Form the feature vector by concatenating the nine LBP features [20].
5. Calculate the best matches using Eq. (12) [21].
6. Retrieve the number of top matches [22].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

B. Similarity Measurement

In the presented work d_1 similarity distance metric is used as shown below:

$$D(Q,I_1)=\sum_{i=1}^{L_g}\left|\frac{f_{L_1,i}-f_{Q,i}}{1+f_{L_1,i}+f_{Q,i}}\right| \quad (12)$$

Where Q is query image, L_g is feature vector length, I_1 is image in database; $f_{1,i}$ is i^{th} feature of image I in the database, $f_{Q,i}$ is i^{th} feature of query image Q.

V. Experiments and Evaluations

When the input data is too large to be processed and redundant, then the input data will be transformed into a reduced representation set of features. Transforming the input data into the set of features is called features extraction [23]. Features extraction involves simplifying the amount of resources required to describe a large set of data accurately [24]. When performing analysis of complex data one of the major problems is the number of variables involved [25].

Here,

$$\Pr ecision(P)=\frac{No.of\ \mathrm{Re}levant\,\mathrm{Im}ages\,\mathrm{Re}trieved}{Total\ No.of\ \mathrm{Im}age\,\mathrm{Re}trieved}x100 \quad (13)$$

$$Group\ \ \Pr ecision\ (GP)=\frac{1}{N_1}\sum_{i=1}^{N_1}P \quad (14)$$

$$Average\ \mathrm{Re}trieval\ \Pr ecision(ARR)=\frac{1}{\Gamma_1}\sum_{j=1}^{\Gamma_1}GP \quad (15)$$

$$\mathrm{Re}call(R)=\frac{Number\ of\ relevant\ image\ retrikeved}{Total\ Number\ of\ relevant\ images} \quad (16)$$

$$Group\ \ \mathrm{Re}call\ (GR)=\frac{1}{N_1}\sum_{i=1}^{N_1}R \quad (17)$$

$$Average\ \ \mathrm{Re}trieval\ \ Rate\ (ARR)=\frac{1}{\Gamma_1}\sum_{j=1}^{\Gamma_1}GR \quad (18)$$

Where N_1 is number of relevant images and Γ_1 is number of groups.

Table 1: Retrieval results of proposed method (GM) and LBP in terms of average retrieval precision (ARP) (%)

Method	Number of top matches considered								
	1	3	5	7	9	11	13	15	16
LBP	100	89.1	84.6	81.7	79.01	76.33	73.86	71.1	69.6
GM	100	93.1	89.7	87.2	85.02	82.71	80.47	77.8	76.4

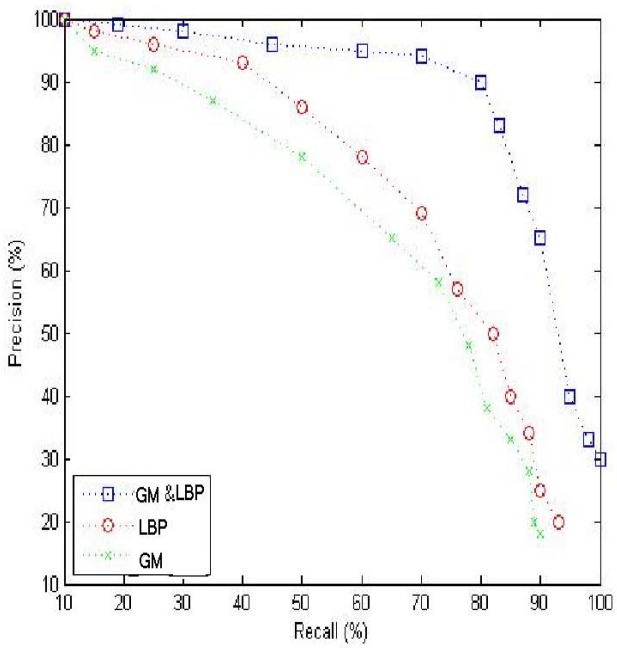


Fig. 5. Average retrieval performance

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Fig .6: Retrieval results using geometrical moments

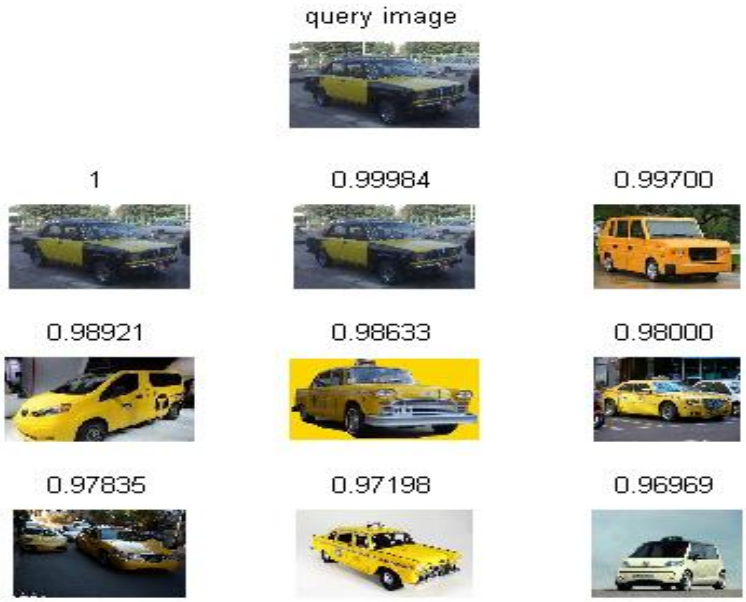


Fig. 7: Retrieval results using LBP

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Fig 8: Retrieval results using combining geometrical moments & LBP

VI. CONCLUSIONS

A new algorithm which is based on the geometrical moments and local binary patterns (LBP) for content based image retrieval (CBIR) is proposed in this paper. The proposed method extracts the nine LBP patterns from a given 3×3 pattern and these are used as the features. Two experiments have been carried out for proving the worth of our algorithm. The results after being investigated shows a significant improvement in terms of their evaluation measures as compared to LBP and other existing transform domain techniques.

REFERENCES

[1] Pietikainen M., T. Ojala, T. Scruggs, K. W. Bowyer, C. Jin, K. Hoffman, J. Marques, M. Jacsik, W. Worek, Overview of the face recognition using feature distributions, Elsevier J. Pattern Recognition, 33 (1): 43-52, 2000.

[2] Rui Y. and Huang T. S., Image retrieval: Current techniques, promising directions and open issues, J.. Vis. Commun. Image Represent., 10 (1999) 39–62.

[3] Ahonen T., Hadid A., Pietikainen M., Face description with local binary patterns: Applications to face recognition, IEEE Trans. Pattern Anal. Mach. Intell., 28 (12): 2037-2041, 2006.

[4] B, A.J., V. P and T. P, . Efficient multimodal biometric authentication using fast fingerprint verification and enhanced iris features. J. Comput. Sci., 7: 698- 706.DOI:10.3844/jcssp, (2011).

[5] Birgale L., Kokare M., Doye D. "Color and Texture Features for Content Based Image Retrieval, International Conf". Computer Grafics, Image and Visualisation, Washington, DC, USA, 146 – 149. 2006.

[6] Brodatz P. "Textures: A Photographic Album for Artists and Designers," New York: Dover. 1996.

[7] Heikkil M., Pietikainen M., A texture based method for modeling the background and detecting moving objects,IEEE Trans. Pattern Anal. Mach. Intell., 28 (4): 657-662, 2006.

[8] M. E , and Y. C, . Fast Extraction of Edge Histogram in DCT Domain based on MPEG7, proceedings of world Academy of Science, Engineering & Technology, volume 9,ISSN 1307-6884, PP. 209-212. (November 2005).

[9] Heikkila M., Pietikainen M., Schmid C., Description of interest regions with local binary patterns, Elsevie J.Pattern recognition, 42: 425-436, 2009.

[10] R. Mukundan, (2004). Some Computational Aspects of Discrete Orthogonal Moments, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 13, NO. 8, AUGUST, 1055, 1059.

[11] Tan X. and Triggs B., Enhanced local texture feature sets for face recognition under difficult lighting conditions, IEEE Tans. Image Proc., 19(6): 1635-1650, 2010.

[12] Beveridge, J.R., She, K., Draper, B.A., Givens, G.H.: A nonparametric statistical comparison of principal component and linear discriminant subspaces for face recognition. In: IEEE Computer Society Conference on Computer Vision and Pattern Recognition.: 535–542., (2011).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[13] Li Zongmin, Kunpeng Hou, Liu Yujie, Diao Luhong and Li Hua, . The shape recognition based on structure moment invariants, International Journal of Information Technology, Vol. 12, No. 2. 2006.

[14] Phillips, P., Grother, P., Micheals, R.J., Blackburn, D.M., Tabassi, E., Bone, J.M.:Face recognition vendor test 2002 results. Technical report (2003)

[15] A. Khotanzad, Invariant image recognition by Zernike moments, IEEE Trans. Pattern Anal. Mach. Intell., vol. 12, pp. 489–497. (Mar 1990).

[16] Zhao, W., Chellappa, R., Rosenfeld, A., Phillips, P.J.: Face recognition: a literature survey. Technical Report CAR-TR-948, Center for Automation Research, University of Maryland,2002.

[17] Sun-Kyoo Hwang and Whoi-Yul Kim,. A novel approach to the fast computation of Zernike moments, Pattern Recognition 39 ,2065 – 2076. 2006.

[18] Hussain, S., Triggs, B.: Feature sets and dimensionality reduction for visual object detection. In: Proc. British Machine Vision Conference, pp. 112.1–112.10 (2010)

[19] He, Y., Sang, N., Gao, C.: Pyramid-based multi-structure local binary pattern for texture classification. In: Proc. Asian Conference on Computer Vision, vol. 3, pp. 1435–1446 (2010)

[20] Chen, J., Zhao, G., Pietikäinen, M.: An improved local descriptor and threshold learning for unsupervised dynamic texture segmentation. In: Proc. ICCV Workshop on Machine Learning for Vision-based Motion Analysis, pp. 460–467 (2009)

[21] Petpon, A., Srisuk, S.: Face recognition with local line binary pattern. In: Proc. International Conference on Image and Graphics, pp. 533–539 (2009).

[22] Yang, H.,Wang, Y.: A LBP-based face recognition method with Hamming distance constraint.
In: Proc. International Conference on Image and Graphics, pp. 645–649 (2007).

[23] Zhang, B., Gao, Y., Zhao, S., Liu, J.: Local derivative pattern versus local binary pattern: Face recognition with high-order local pattern descriptor. IEEE Trans. Image Process. 19(2), 533–544 (2010).

[24] Zhu, C., Bichot, C.-E., Chen, L.: Multi-scale color local binary patterns for visual object classes recognition. In: Proc. International Conference on Pattern Recognition, pp. 3065–3068 (2010).

[25] Zhao, S., Gao, Y., Zhang, B.: Sobel-LBP. In: Proc. International Conference on Image Processing, pp. 2144–2147 (2008)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

An Efficient Modeling and Simulation of Quantum Key Distribution Protocols Using OptiSystem™

Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K.Subramaniam
FSKTM
University Putra Malaysia
Serdang, Malaysia

Hishamuddin Zainuddin
INSPEM
University Putra Malaysia
Serdang, Malaysia

Suhairi Saharudin
MIMOS BERHAD
Technology Park Malaysia
KL, Malaysia

Abstract— **In this paper, we propose a modeling and simulation framework for quantum key distribution protocols using commercial photonic simulator OptiSystem™. This simulation framework emphasize on experimental components of quantum key distribution. We simulate BB84 operation with several security attacks scenario and noise immune key distribution in this work. We also investigate the efficiency of simulator's in-built photonic components in terms of experimental configuration. This simulation provides a study to analyze the impact of experimental photonic components in quantum key distribution process.**

Keywords-quantum cryptography; qkd-simulation;optisystem;

I. INTRODUCTION

Secure key distribution is one of the intrigue researches in the network security field. Digital cryptography affords a solution based on computational security. As today's rapid technology growth is capable of breaking the security by a simple technique called brute force attack in near future. Furthermore the imminent product from quantum mechanics (QM) principle is the quantum computer and its algorithms are capable of solving the non polynomial (NP) problem in polynomial time. On the other hand, quantum cryptography from QM offers an unconditional security by its uncertainty principle, no-cloning theorem and entanglement.

Many researches have been done on QC area so far. As a result, start from BB84 [1] the ground-breaking quantum key distribution (QKD) protocol until recent QLE-1 [2], QC transforms into matured field of quantum mechanics. Unlike quantum computer, quantum key distribution (QKD) protocols are already available in the market.

QKD is a combination of hardware (i.e. photonic and optical telecom components) and software (protocols & post quantum methods) to accomplish the unconditional key distribution. The intrinsic property of QKD is the detection of eavesdropping makes it a hefty application.

Most researches on QKD are analytical oriented and few only are experimental. Due to the impact of cost, the experimental type researches are few. On the other hand, an analytical or mathematical research has numerous limitations which affect the efficiency of the results. This research usually ignores the importance of hardware. In other words, consideration of the affect of hardware in QKD by analytical research is insignificant. Additionally, for the fresh researchers to understand the QKD operation makes difficult. On contrast, understanding the digital cryptography or digital network protocols are simple due to the availability of simulation option. These researches not only have efficient analytical or experimental researches but also they have effective simulation. In particular, discrete event simulation on network protocols are de facto standard for evaluating the performance metrics.

To study and evaluate the quantum computers and its algorithms various methods are available. The options ranges from new functional programming language, library for high-level language, online services, framework, interactive simulation, GUI oriented - circuit oriented simulators, emulators and visualization [3]. On the other hand, to study the QKD operations are very few and inefficient.

II. RELATED WORKS

In this Section, we analyze related works which are focus on QKD simulation. Before probe into literature, we give a short glimpse of QKD operation in the following table.

TABLE I. QKD ENTIRE OPERATIONS

Stage	Procedure	Channel
1	Qubits Exchange	Quantum
2	QBER/Sift	Public
3	Error Correction	Public
4	Privacy amplification	Public

From above table except qubits exchange all other procedures are performed in public channel. This is a two party system conventionally called Alice and Bob as the legitimate users and Eve is an illegitimate user. Our proposed simulation framework concentrates on stage 1. Other stages i.e. sifting, error correction and privacy amplification are also called post-quantum action or key distillation process. These actions are required to establish secure key where Eve has a negligible knowledge on the secret key.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Attila Pereszlényi's Qcircuit which studies the QKD protocols by means quantum circuit level. Qcircuit has quantum circuit interface with various objects to denote the OKD elements and analyze quantum bit error rate (QBER) [4]. Object oriented simulation for QKD was proposed by Xiufeng et al [5]. Shuang and Hans proposed an event-by-event simulation model [6] and polarizer as simulated component for QKD protocols i.e. BB84 and Ekert[7] with presence of Eve and misalignment measurement as scenarios. Reference [8] presented a C++ application to evaluate and test quantum cryptography protocols. This application has elegant user-friendly interface and many modules which complete entire QKD operations. It includes BB84 and B92 as a protocol options; two modules for eavesdropping; a noise level module; and privacy amplification. This simulation suited for understanding overall QKD operations. In contrast to above works, our proposed simulation concentrates more on experimental elements. Further, scalability of our module is better. One can extend to other encoding i.e. phase, amplitude and deployment of decoy states. However entangled based QKD and correlation of simulation output statistics with published experimental results are still upcoming challenges. Moreover, QKD field is still lacking of efficient simulation to study and evaluate the hardware performances.

In this paper, we propose our modeling and simulation framework and we simulate the BB84 with Eve's attacks scenario and noise immune QKD protocols using the OptiSystem™ simulator.

III. Proposed Modelling and Simulation Framework

OptiSystem™ 7.0 [9] software provides variety of optical communication modeling and simulation. It has most of the photonic telecom components. Let us come to our objective, modeling QKD experiments using the OptiSystem™ looks simpler in shallow, but in deep their in-built components are not correlated with QKD operation. For instance, polarization beam splitter (PBS) is one of the important passive components of the QKD; its basic operation is to pass the incoming light based on its angle. Unfortunately, in optiSystem™, PBS splits the incoming light into two different angles. Such a way, some of the available components in the OptiSystem™ components library not execute as QKD components. For these cases, we need alteration or create new components to rectify it. However, OptiSystem™ has some other built in libraries can be utilized for simulation called visualizers. Under this library, we can use polarization analyzer and power meter components for photon counting as well as detectors.

In telecommunication experimental scenario, there are three major classifications namely transmitter, channel, and receiver. We can relate this paradigm to the QKD protocols. In transmitter block, photon source is an important component and OptiSystem™ offers wide variety of optical sources with many intrinsic properties. Attenuation is a vital mechanism in QKD for getting single photon level from photon pulses. Polarizer is another important passive component for polarizing the photon in desired angle. For the channel classification, optical fiber is the standard component and fully support by the simulation software.

As we mentioned earlier the problem of PBS, to overcome this problem OptiSystem™ offers a simple solution. The component called 'select' can be used as PBS as well as random selection of the incoming photons. Usually, in QKD experiments sender randomly choose the polarization to send the photons to receiver. Receiver also picks random polarization for measuring the incoming photon. This mechanism also carried out by the select component itself. Finally based on the polarization, detectors will trigger. The sender and receiver record all photons value for discussing in the public channel. The following Fig. 1 explains the basic operation of the QKD scenario explained.

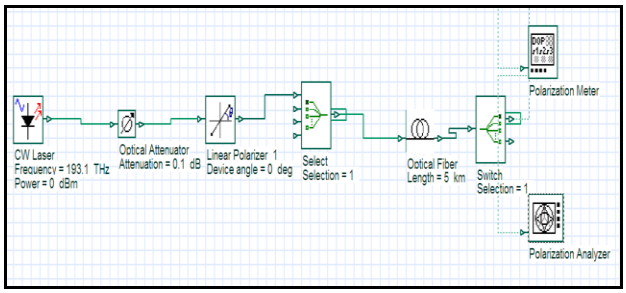


Figure 1. Basic QKD setup

In this above figure, instead of detectors like PD(Avalanche Photo Diode), we use the another components called polarization analyzer which shows the value of polarization (both azimuth and ellipticity) and polarization meter is an optional component to measure the power. At this point, detector is not implemented in our simulation.

Another vital concern is about the randomness. In our simulation model, only 'select' component requires randomness. Most of the component in OptiSystem™ has in-built property called sweep calculation. This allows simulation to perform much iteration with different set of values. For randomness, we utilize discrete function consist of random seed index, minimum value, maximum value and delta parameters. By carefully choose the right values for these parameters, good randomness can be achieved. Random values are passed the frequency test from NIST suite [10].

A. BB84 Protocol Simulation

In the following Fig.2, we illustrate the complete operation of BB84 protocol. This experimental model is slightly modified from the original QKD practical setup [11].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

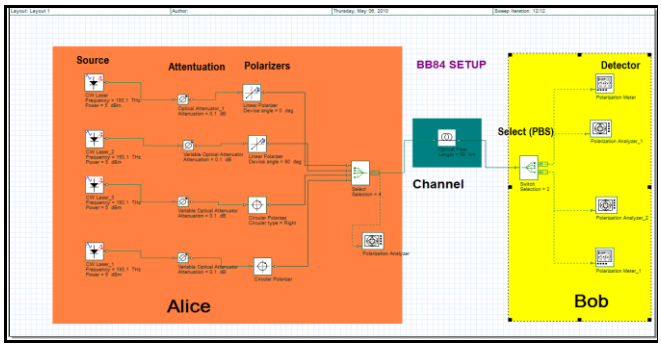


Figure 2. BB84 Protocol Mechanism

In the Fig. 2, we implement four coherent wave optical sources (CW laser) with variable optical attenuator (VOA) with attenuation value 0.1 to have single photon. We also set four type of polarizer namely horizontal, vertical, left diagonal and right diagonal. We run at least 2000 iterations, for each iteration, component 'select' is to choose a qubit randomly out of four polarization angles and pass through the optical fiber to the receiver side. On receiver side, we implement again select component to simulate the randomness of selecting the linear polarization or diagonal polarization and detection done by the polarization analyzer. This is the simple setup for basic BB84 operation. OptiSystem™ comes with wide option to export the data to files, excel and Matlab. Our simulation also consist a small visual basic script (vbscript) to extract both sender's and receiver's polarization analyzer values to excel. Finally, simple calculation to get quantum bit error ratio (QBER) value. The visualizer output is showed as Fig. 7 and Fig. 8 in Appendix.

B. BB84 Operation with Eve's Attacks

1) Eve's Capabilities

Eve could ever perform against the quantum channel, assuming Eve has absolutely no technological limits, i.e. she can do everything that quantum physics does not explicitly forbid. But, clearly, Eve's attacks are not limited to the quantum communication channel. For instance, Eve could attack Alice or Bob's apparatuses, or she could exploit weaknesses in the actual implementation of abstract QKD. Reference [8-18] indicate various security attacks. Our simulation utilize simple model of combination of attacks.

Mostly, Eve's attacks are classified as individual, coherent and incoherent attacks. For our experiment we generalize the Eve's attack mostly based on Intercept-Resend attack strategy and man-in-middle attack. Further, Denial of Service (DoS) attack is performed in our simulation. We assumed DoS carried out by Eve by simply abort the transmission line between Alice and Bob. This scenario particularly suits in fiber optic channel. In our experiment scenario, Eve is the connection hub between Alice and Bob. She can do various actions to obtain the key, or simply deny the transmission. Eve's different security attacks on BB84 protocol is illustrated in Fig. 3 and Fig. 9 (Appendix section shows in full view size). Further, Fig. 7 and Fig. 8 represent detector attributes in which we analyze the signal's polarization by frequency and Poincare sphere analysis.

Eve can do intercept on incoming qubits and measure with rectilinear, diagonal polarizers, phase shift, photon rotator. She can send a new qubit to Bob. Further, She can also send null qubit or Alice's qubit to Bob. We use 'select' component for Eve's random attacks. Finally we calculate the QBER based on Alice , Eve and Bob measurements. The total number of sweep iteration is 10000.

Table – II represents the generalized result of the Eve's attacks on BB84 and table head notations i.e. PZ refers polarization, H, V and D denotes to horizontal, vertical and diagonal polarizer and 'Action' column indicates decision made by Alice and Bob after exchange qubits.

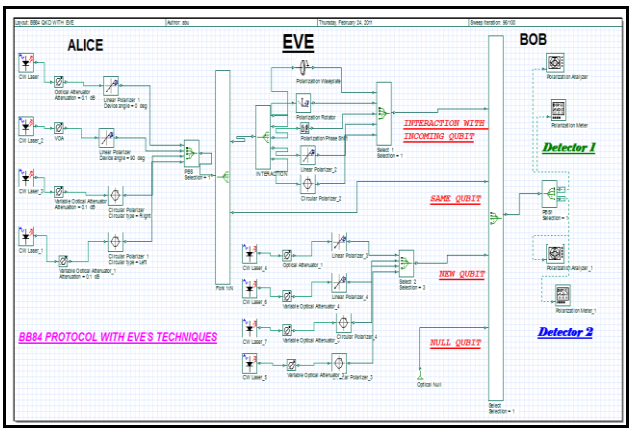


Figure 3. BB84 Operation with Eve's Attacks

TABLE II. GENERALIZED RESULT -BB84 WITH EVE'S ATTACKS

Sender		**Receiver**		**Eve**		**Action**
PZ	***Bit***	***PZ***	***Bit***	***Attack***	***Bit***	
H	0	H/V	0	Nil	-	Sift Key
V	1	H/V	1	Nil	-	Sift Key
D	0	D	0	Nil	-	Sift Key
D	1	D	1	Nil	-	Sift Key
H/V	0/1	D	<?|	Nil	-	Discard
D	0/1	H/V	<?|	Nil	-	Discard
H/V	0/1	H/V	0/1	Intercept Resend (H/V)	0/1	Sift Key
H/V	0/1	H/V	<?|	Intercept Resend (D)	<?|	QBER
H/V	0/1	D	<?|	Intercept Resend (H/V)	0/1	Ignore
D	0/1	D	<?|	Intercept Resend (H/V)	<?|	QBER
H/V-	0/1	H/V	<0/1| /<?|	Intercept Resend II (H/V)/ D	<0/1 > <?>	Sift Key / QBER
D	0/1	D	-	DoS	-	No Action
(H/V) D	0/1	(H/V) D	</0/1> <?|	DoS	-	Receiver's Detector Dark Count

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C. Noise Immune QKD

In our second experiment, we simulate noise immune QKD. Noise is considered one of the biggest challenges in QKD. Distinguishing noise from eavesdropping is an intrigue research. Noise can come various components, from fiber optic channel i.e. birefringence, polarization dispersion and free space issues i.e. scattering, absorption, diffraction, etc. Further, detectors problems like dark count and detection efficiency. As summarize, noise has various triggering factors which results in poor performance in QKD especially in secure key generation rate and distance. There have been several solutions proposed by researches. We implement one of experiment and briefly explained its protocol.

Bob sent rectilinear basis photon to Alice. Alice passes incoming qubit to faraday rotator and forward to Bob. Alice also sent unpolarized photon to Bob. The information about photon is calculated by the polarization basis and time delay between photon. For further information about the protocol refer [19].

The property of faraday rotator is given by the following property.

$$H_{in} \rightarrow \text{Faraday Rotator} \rightarrow V_{out}$$
$$V_{in} \rightarrow \text{Faraday Rotator} \rightarrow H_{out}$$

Here H and V refer to horizontal and vertical basis. In our simulation, we use polarization rotator which is inbuilt OptiSystem's component. The noise immune qkd simulation is showed in Fig.10 and the optical fiber properties are depicted in Fig.8. Fig.11 and Fig.8 are available in appendix section.

Polarization rotator's property,

$$0^\circ - 90^\circ = -90^\circ$$
$$90^\circ - 90 = 0^\circ$$

Here 0° and 90° refer to rectilinear angles. We utilize two 'Time Delay' components for time difference between photon sent. Both components generate time/value based on value from pseudo random number generator. This is implemented by simple VbScript expression in sweep iteration. For detectors, we used photon analyzer and all data are transferred to Excel sheet using VbScript. The Table. III elaborates generalized result of this experiment. The total number of iteration is 10000.

TABLE III. GENERALIZED RESULT- NOISE IMMUNE QKD

Sender's Parameters			***Receiver's Parameters***	***Result***	
Sent Photon	***Received$_{Photons}$***		***Time Delay***	***Status***	***Bit***
	1st Photon	***2nd Photon***			
H	V	Unpolarized	No	Accept	0
V	H		No	Accept	0
H	Unpolarized	V	Yes	Accept	1
V	Unpolarized	H	Yes	Accept	1
H	H	Unpolarized	No	Ignore	-
V	V	Unpolarized	No	Ignore	-
H	V	-	No	Ignore	-
V	H	-	No	Ignore	-

IV. RESULTS AND DISCUSSIONS

In this section, we highlight some results from the simulation setup. Fig. 4 and Fig. 5 represent the results from the BB84 simulation protocol and noise immune key distribution result is shown in the Fig. 6

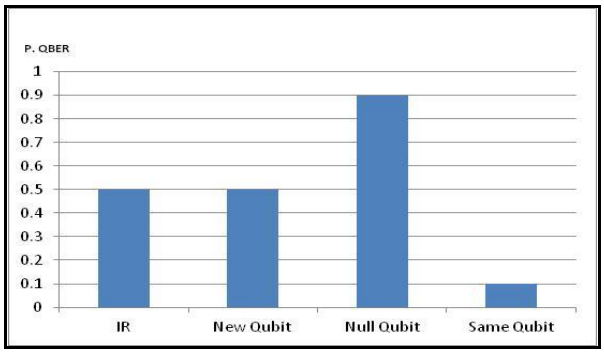


Figure 4. Probability of QBER by Eve's Action

Fig. 4, shows the probability of QBER by attacks done by Eve. The intercept and resend attack cause 0.5 probability of QBER. This is due to randomness of selecting qubit by Eve. Eve can cause 50% chances of choosing different polarizer. The highest probability of QBER is done by null qubit. In our simulation setup, it contributes 0.9 probability for QBER. This attack can easily be detected by legitimate parties using the clock event. Null qubit can be unpolarized light. If Eve, allows the same qubit generated by Alice and Bob chooses correct polarizer, then it contributes lowest QBER. In our simulation, 0.1 probability of error is added for the detector inefficiency..

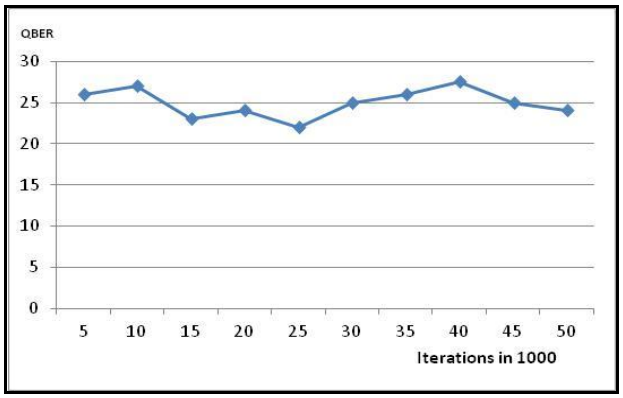


Figure 5. BB84 with Eve's Attack Scenario Simulation Result

Fig. 5 shows overall the QBER on each iteration. The average is 25% of QBER. This indicates the presence of Eve is strong and explicit. As we mentioned earlier, our randomness passed through the frequency test. Thus, each iteration differed from each other. The overall QBER range is from 22% to 28%.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

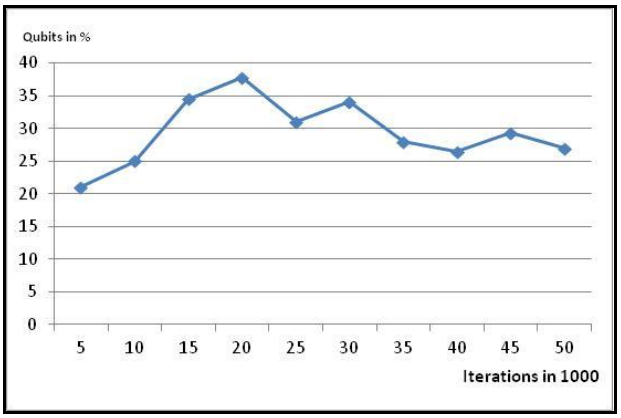


Figure 6. Noise-immune QKD simulation result

Fig. 6, illustrates the percentage of discarded qubits in the simulation setup. In this experiment, no Eve module included and assume that ideal channel and ideal receiver. Our simulation results show the range from 20-38% qubits discarded in the simulation. The graph has much fluctuation to emphasize the randomness set-up of the simulation. Implicitly, result show for higher key rate than the experimental setup. More than 65% of qubits can be used for key generation. In experimental case, around 25% qubits support in key generation.

V. CONCLUSION

Most QKD simulation researches focused on protocol mechanism. Our study focuses on hardware setup based on OptiSystem™. As we mentioned earlier, QKD is a combination hardware and protocol paradigm to achieve unconditional security in key distribution. Both paradigms should be evaluated correctly to understand and study the performance of QKD protocols efficiently. Our proposed simulation framework emulates the practical experiments with slightly modified components. We can modify the parameter settings of the components and able to find the optimum value. Thus, this simulation framework reduces the implementation cost by choosing appropriate components' property. This simulation setup still needs vigorous testing and analysis. Implementation of entanglement oriented and other encoding based QKD are the challenges for the future work.

REFERENCES

[1] C.H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Bangalore, India.

[2] http://www.quintessencelabs.com/

[3] http://www.quantiki.org/wiki/List_of_QC_simulators

[4] A. Pereszlenyi, "Simulation of quantum key distribution with noisy channels."

[5] X. Zhang, Q. Wen, and F. Zhu, "Object-Oriented Quantum Cryptography Simulation Model," IEEE, pp. 599-602.

[6] S. Zhao, and H. De Raedt, "Event-by-event Simulation of Quantum Cryptography Protocols," *Journal of Computational and Theoretical Nanoscience,* vol. 5, no. 4, 2008, pp. 490-504.

[7] A.K. Ekert, "Quantum cryptography based on Bell's theorem," *Physical Review Letters,* vol. 67, no. 6, 1991, pp. 661-663.

[8] M. Niemiec, Ł. Romański, and M. Święty, "Quantum Cryptography Protocol Simulator," *Multimedia Communications, Services and Security*, 2011, pp. 286-292.

[9] http://www.optiwave.com/

[10] http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

[11] H. Zbinden, N. Gisin, B. Huttner, A. Muller, and W. Tittel, "Practical Aspects of Quantum Cryptographic Key Distribution," *Journal of Cryptology,* vol. 13, no. 2, 2000, pp. 207-220.

[12] C. Branciard, N. Gisin, N. Lutkenhaus, and V. Scarani, "Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography," *Arxiv preprint quant-ph/0609090*, 2006.

[13] Q.Y. Cai, "Eavesdropping on the two-way quantum communication protocols with invisible photons," *Physics Letters A,* vol. 351, no. 1-2, 2006, pp. 23-25.

[14] M. Curty, L.L. Zhang, H.K. Lo, and N. Lütkenhaus, "Sequential attacks against differential-phase-shift quantum key distribution with weak coherent states," *Arxiv preprint quant-ph/0609094*, 2006.

[15] J. Anders, H.K. Ng, B.G. Englert, and S.Y. Looi, "The Singapore Protocol: Incoherent Eavesdropping Attacks," *Arxiv preprint quant-ph/0505069*, 2005.

[16] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," *Journal of Modern Optics,* vol. 48, no. 13, 2001, pp. 2009-2021.

[17] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A,* vol. 73, no. 2, 2006, pp. 022320.

[18] 18. W.H. Kye, and M.S. Kim, "Security against the Invisible Photon Attack for the Quantum Key Distribution with Blind Polarization Bases," *Arxiv preprint quant-ph/0508028*, 2005.

[19] Walton, Z., et al., *Noise-Immune Quantum Key Distribution.* Quantum communications and cryptography, 2006: p. 211.

APPENDIX

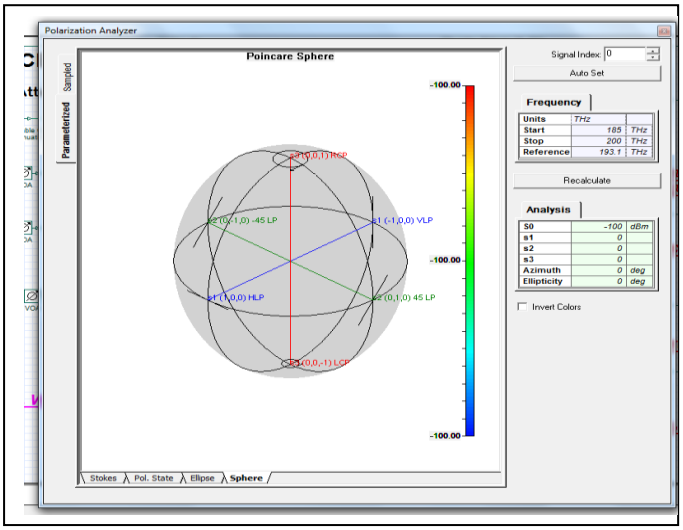


Figure 7. Detector's attributes- Poincare Sphere

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

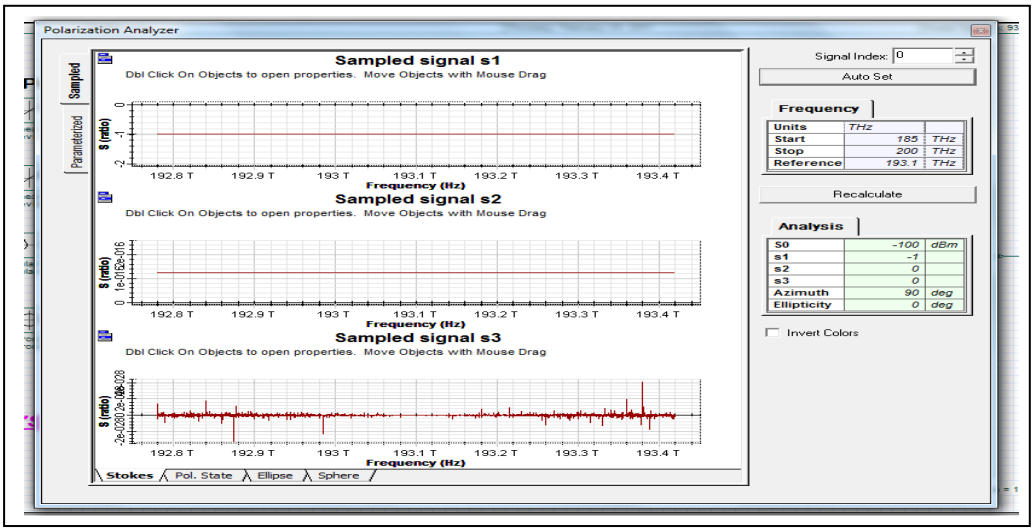


Figure 8. Detector's attributes – Frequency analysis

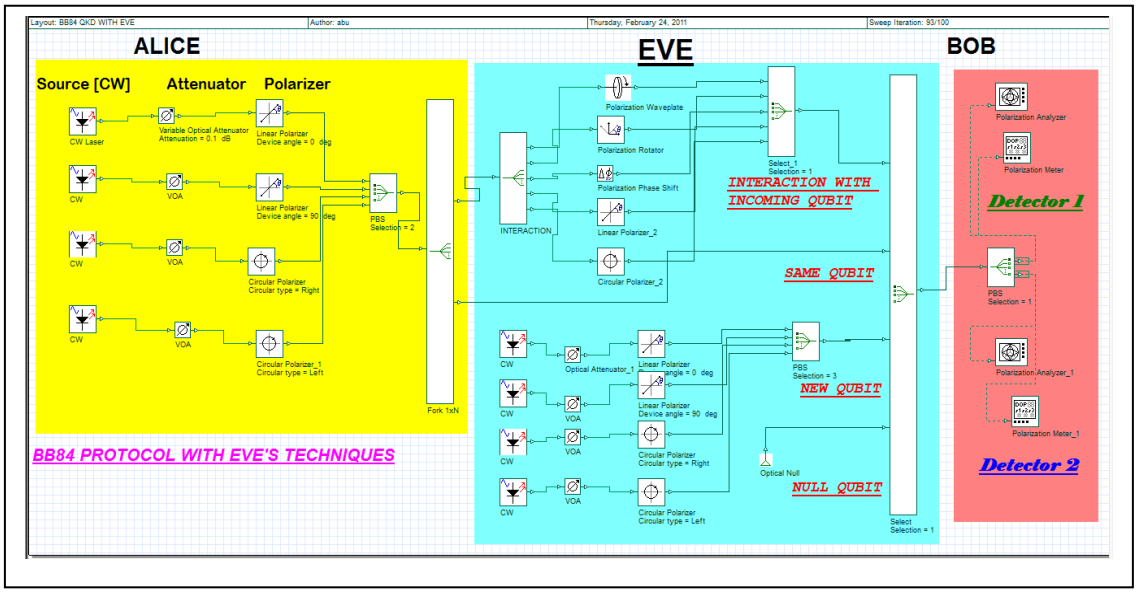


Figure 9. BB84 with Eve's Attacks (same as Fig.3)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

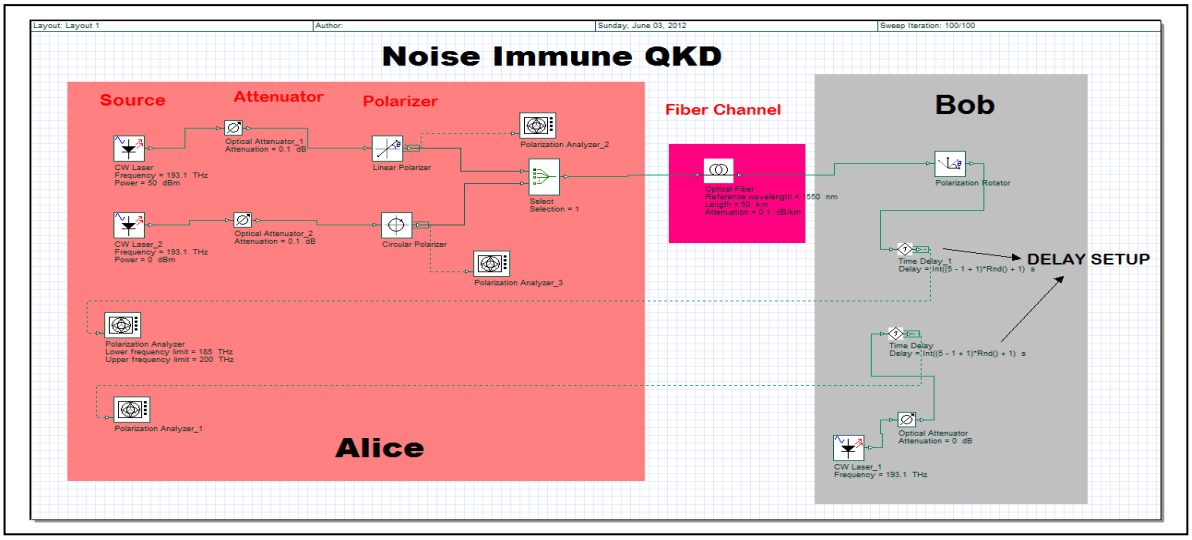


Figure 10. Implementation of Noise Immune QKD

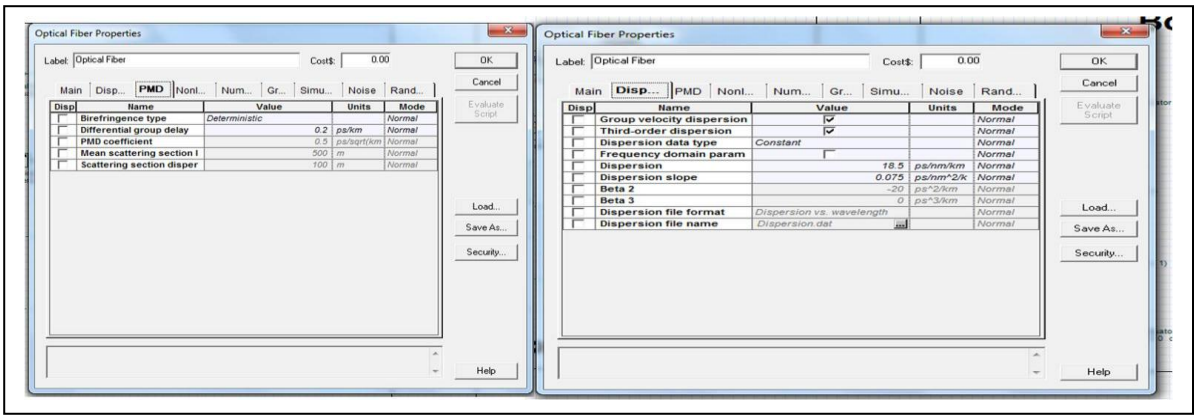


Figure 11. Optical Fiber Properties Simulation Window

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Investigation of Security Enhancement and Performance Attributes of Key Agreement Protocol in Elliptic Curve Cryptography

Sonali U Nimbhorkar
Computer Science &Engineering
G.H.Raisoni College of Engineering
Nagpur, India
sonali.nimbhorkar@raisoni.net

Dr.L.G.Malik
Computer Science & Engineering
G.H.Raisoni College of Engineering
Nagpur, India
latesh.malik@raisoni.net

***Abstract*—Augmented network use to communicate susceptible data and transactions requires an enhanced level of authentication and privacy for digital communication .Now a day's most of the user authentication, integrity and confidentiality schemes are based on elliptic curve cryptography. The use of elliptic curve cryptography techniques provide greater security using less bits .The construction of key agreement protocol in elliptic curve cryptography requires being resistant to both active and passive attacks. In this paper provides comparative cryptanalysis of vulnerable schemes for key agreement protocol using elliptic curve cryptography and also considering parameters for security enhancement and performance attributes for achieving greater security for communication networks reducing computational overhead, bandwidth, and storage requirement.**

Keywords—Key agreement ,elliptic curve , finite field , security, cryptosystem .

I. INTRODUCTION *(HEADING 1)*

In cryptography, a key agreement protocol is a protocol whereby two or additional parties can agree on a key in such a way that both control the outcome .Key agreement protocols are considered one of the hardest protocols to design, and are one of the most important parts of a system when it comes to integrity and confidentiality of data. Many key agreement protocols have been proposed, but many of them are without security proof. Even with the security proof, the protocol may contain weaknesses that may be exploited with a new kind of attack. Because of this, it must continuously analyze protocols to make sure that they are sound. Key agreement protocols are the common way for two principals to achieve secure communication by establishing a session key to encrypt the data that is being sent between them[8][9][15].

A secure key agreement protocol should be enforced while two parties communicate to each other to defend themselves from various kinds of active and passive attacks .There are two basic models for secure key agreement protocols one is Authenticated key(AK) and another is Authenticated key with key confirmation (AKC)[10][11].

Key establishment protocols have conventionally been among the hardest protocols to design. There are several challenges concerning key exchange. These are:[17][19]ensuring that the keys are exchanged so that sender and receiver can perform Encryption and decryption, preventing an eavesdropper from getting to know the key, offer the receiver ,some proof that a message was encrypted by the party who claims to have sent the message. The rapid growth in communication technology and personal communication systems encouraged new security questions.

Recently commencing 2002 to 2012, many studies were proposed to secure authentication protocols. In2008,.numerous schemes proposed an improved key agreement protocol [6] [8][19] [27] [28]. These protocol is a smart card based password authentication protocol and operates with symmetric key encryption algorithm. They claimed that their protocol is secure, can achieve user anonymity, and prevent various attacks, such as replay attack, stolen verifier attack, password guessing attack, insider attack, and man-in-the-middle attack. In 2009, proposed a scheme [11][26] which is improved protocol [26] and can avoid the weakness existing in protocol is also a smart card based password authentication protocol and bases on bilinear pairings. They claimed that their protocol is secure and can withstand replay attack and insider attack and also proposed an improvement on protocol [11]. Their scheme is a smart card based password authentication protocol as well and operates with secure one-way hash function. They claimed that their protocol is secure and can achieve mutual authentication. Also in 2011, improved two identity-based authentication protocols, [2] [3][5][13][16][30][34][40]. Their protocols are r password-based smart card based protocols. They are identity-based public key cryptosystem and operate with ElGamal signature scheme. Claimed the protocols are not only efficient but also secure. Although all of the above schemes mentioned claimed

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that they are secure, however, there are still some threats existing in them.

The rest of the paper is organized as follows. Related Works and Fundamental required for key agreement protocol are briefly discussed in Section II. Desirable properties of key agreement protocols are given in Section III. Section IV presents various attack methods For key agreement protocol, security analysis with respect to key agreement properties and possible attacks. Performance comparison with respect to design schemes for key agreement protocol and other related schemes is given in Section V. Finally conclude the paper in Section VI.

II. FUNDAMENTALS OF FOR KEY AGREEMENT PROTOCOL

There are three major categories of key agreement schemes defined in the standards with two of these categories having multiple cases [14][15][16]:

- Two-Party Participation: an interactive, two-way method where each party generates an ephemeral key pair. This method is used in the most widely deployed security protocols.
- One-Party Participation: a store-and-forward, one-way method where only the initiator generates an ephemeral key pair. This method is ideally suited to email and is used in the S/MIME protocol. It can also be used in SSL if the server has a static DH public-key.
- Static Keys Only: a static (passive) method where each party has only a static key pair, no ephemeral keys are used. This method can be used in S/MIME and SSL but the absence of ephemeral keys diminishes its security. In this method, the shared symmetric keys are only assured to be distinct from previous by adding unencrypted (public) nonce's to the derivation of the shared keys.

In addition, two important properties are regarded for key agreement protocols as follows [14][16]:

- Implicit key confirmation: A key agreement protocol has this property if the both participants are assured that only the other participant can compute the secret common key.
- Explicit key confirmation: This means that the both participants are assured that the other participant have computed the secret common key.

III. DESIRABLE PROPERTIES OF KEY AGREEMENT PROTOCOLS

A number of desirable properties for key agreement protocols have been identified [2] and nowadays most of the protocols are analyzed using these properties which are described below [17][19][26]:

- Known-key security: Each run of a key agreement protocol between two entities A and B should produce a unique shared secret key called session key Ks. A protocol should still achieve its goal in the face of an adversary who has learned some other session key.
- Perfect forward secrecy: If long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities is not affected.
- Key-compromise impersonation: Suppose that A's long- term private key is disclosed. Clearly an adversary that knows this value can now impersonate A, since it is precisely this value that identifies A. However, it may be desirable that this loss does not enable an adversary to impersonate other entities to A .In addition, Identification protocols should have other properties which are related to performance. Because round trips and large blocks are critical factors in terms of communication load and because exponentiations and random numbers are to be critical factors in terms of computation load.
- Computational efficiency: this includes the number of operations required to execute a protocol. In order to achieve this property, the protocol should have the minimum number of operation as possible.

Communication efficiency: This includes the number of passes (message exchanges) and Communication efficiency: This includes the number of passes (message exchanges) and the bandwidth required (total number of bits transmitted).

IV. ATTACK METHODS FOR KEY AGREEMENT PROTOCOL

There are numerous different ways to perform an attack on a key agreement protocol. In this will briefly depict how attacks may be characterized, the distinction between active and passive attacks and present some widespread attack methods. There are many different ways an attacker can develop a protocol This section contains a brief description of some of the most common attack methods [28][1][4] :

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- **Eavesdropping:** Eavesdropping means that an adversary captures information that is being sent in the protocol. Eavesdropping has existed throughout time, where someone overhears things they were not supposed to and when the communicating parties are not aware of it. This is one of the most basic kinds of attack, and more complex attacks might include eavesdropping as part of the attack. Eavesdropping is a kind of passive attack.

- **Modification:** In a modification attack, the adversary alters the information that is sent in the protocol. This is a kind of active attack, since the attacker has a stronger role in this situation than a passive attack, where he just listens to the communication. A way to prevent this kind of attack is to use cryptographic integrity measures.

- **Replay:** A replay attack is an attack where a valid transmission is being recorded, and then later repeated, to the same or a different principal, for attacking purposes. This is done either by the originator or by an adversary who intercepts the data and retransmits it. This is a fundamental kind of attack, which is often used as a part of more complex attacks. One way to avoid replay attacks is using session.

- **Reflection:** A reflection attack is a way of attacking a challenge-response authentication system that uses the same protocol in both directions. The idea is to trick the target into providing the answer to its own challenge. This attack is only possible if the protocol allow parallel runs. The way to prevent this attack is to require the initiating party to first respond to challenges before the target party responds to its challenges.

- **Denial of service attack:** A denial of service attack is when attackers send many invalid requests to a server without establishing a server connection in order to overwhelm a server and stop legitimate users from getting a connection with the server.

- **Typing attack:** A typing attack means that the adversary replaces a message field of one type with a message field of another type. This will make the recipient is interpret a message, and accept a protocol element as another one (of a different type). For Example could a principal identifier be falsely accepted as a key.

- **Cryptanalysis:** Cryptanalysis is the study of methods for obtaining the meaning of encrypted information, without access to the secret information that is normally required. In most cases, this kind of attack focuses on finding the secret key. Frequency analysis is the basic tool for breaking classical ciphers and reveals the secret key.
- **Certificate manipulation:** Certificate manipulation is when the adversary modifies certificate information to perform an attack on a protocol. The certificate of a principal acts as an assurance from a trusted third party that the principal's public key really does belong to that principal.
- **Protocol interaction:** Protocol interaction means that the adversary chooses a new protocol to interact with a known protocol. Most of the long-term keys are meant to be used for a single protocol only.

V. DESIGN SCHEMES FOR KEY AGREEMENT PROTOCOL

Design methods used for designing the new key agreement protocols are based on some standard protocols. Here we describe the most important of these standards. Also present the assumed problems that is used in cryptography in order to keep information available to the intended parties, and unavailable to others [24][26][28].

a) Diffie-Hellman key agreement protocol

Diffie-Hellman is a cryptographic protocol for secure exchange of a shared secret between two parties over an untrusted network. The two parties may not have ever communicated previously, but with their new shared secret key they can encrypt their communications over the insecure channel. The perhaps most important part of the protocol is that the key is not sent over the connection, so that it can be detected by an Eavesdropper [24][28]

b) Elliptic Curve Cryptosystems

Elliptic curve cryptography depends on the difficulty of solving the discrete logarithm for the group of an elliptic curve over some finite field. This problem is called Elliptic Curve Discrete Logarithm Problem, ECDLP [13][9][25].

c) MQV protocol:

This protocol is used to establish a shared secret between two parties. Both parties generate dynamic private/public key pairs and exchange their public keys. Then each party calculates an implicit signature by using his own private key and the other party's public key. This signature is used to generate the shared secret. The secret generated by each party will be the same only if they are based on the corresponding public keys [25][26][30].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. CONCLUSION

It has been seen that public key based on key agreement protocol provides strong mean for authentication, data integrity and non-repudiation .This paper provides an introduction to Elliptic Curves and how they are used to create a secure and powerful cryptosystem. Elliptic curve cryptography provides a methodology for obtaining high-speed, efficient, and scalable implementations of network security protocols. The achievement on the protocol goals and the complete security analysis parameters are also consider overcoming the known security flaws from communication network.

REFERENCES

[1] Eun-Jun Yoon1, Sung-Bae Choi2 and Kee-Young Yoo3*"* A Secure And Efficiency Id-Based Authenticated Key Agreement Scheme Based On Elliptic Curve Cryptosystem For Mobile Devices**"** International Journal of Innovative Computing, Information and Control ICIC International c 2012 ISSN 1349-4198 Volume **8**, Number **4**, April 2012 pp. 2637-2653 .

[2] Kavitha Ammayappan , Atul Negi , V. N. Sastry and Ashok Kumar Das" An ECC-Based Two-Party Authenticated Key Agreement Protocol for Mobile Ad Hoc Networks" JCP110116219-KNSD,2011.

[3] Ja'afer M. AL-Saraireh, Mohammad S. Saraireh" Formal Analysis of A Novel Mutual Authentication and Key Agreement Protocol" Applied Science University11961, Jordan.JCS&T Vol. 11 No. 2 October 2011.

[4] M. Aydos, E. Sava¸s, and C¸ . K. Ko¸c "Implementing Network Security Protocols based on Elliptic Curve Cryptography *"*Proceedings of the Fourth Symposium on Computer Networks, S. Oktu˘g, B. ¨ Orencik, and E. Harmancı, editors, pages 130–139, Istanbul, Turkey, May 20-21, 1999.

[5] A. Katvickis, E. Sakalauskas, N. Listopadskis" Microprocessor Implementation of Key Agreement Protocol over the Ring of Multivariate Polynomials" *ISSN 1392 – 1215 2011. No. 10(116).*

[6] P. Vijayakumar ,V. Vijayalakshmi "Effective Key Establishment and Authentication Protocol for Wireless Sensor Networks Using Elliptic Curve Cryptography" Mobile and Pervasive Computing (CoMPC–2008)

[7] B.Maheshwari," Secure Key Agreement And Authentication Protocols" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.3, No.1, February 2012DOI: 10.5121/ijcses.2012.3111 113.

[8] Liufei Wu,Yuqing Zhang, Fengjiao Wang " A New Provably Secure Authentication and Key Agreement Protocol for SIP Using ECC " IEEE 2008 .

[9] Atishay Bansal, Dinesh Sharma, Gajendra Singh, Tumpa Roy" New Approach For Wireless Communication Security Protocol By Using Mutual Authentication "Advanced Computing: An International Journal (ACIJ), Vol.3, No.3, May 2012 DOI : 10.5121/acij.2012.3303 31 IEEE.

[10] He Debiao*, Chen Jianhua, Hu Jin" Weakness of two ID-based remote mutual authentication with key agreement protocols for mobile devices" International Conference on Computational Science and Engineering, 2010 IEEE.

[11] Yoon E.-J., Yoo K.-Y., Robust "ID-based Remote Mutual Authentication with Key Agreement Protocol for Mobile Devices on ECC, 2009 International Conference on Computational Science and Engineering, 2009, pp. 633-640.,IEEE

[12] Ja'afer AL-Saraireh & Sufian Yousef **"**Extension of Authentication and Key Agreement Protocol (AKA) for Universal Mobile Telecommunication System (UMTS)"International Journal of Theoretical and Applied Computer Sciences Volume 1 Number 1 (2006) pp. 109–118 (c) GBS Publishers and Distributors (India) 2006.

[13] Debiao He."Weakness in a Mutual Authentication Scheme for Session Initiation Protocol using Elliptic Curve Cryptography" 1108.4076,(2011).IEEE.

[14] Kaiping Xue, Peilin Hong, Changsha Ma "A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture" arXiv:1204.3831v1 [cs.CR] 17 Apr 2012.

[15] Hassan Keshavarz, Mohammad Reza Jabbarpour Sattari and Rafidah Md Noor " Session Initiation Protocol Attacks and Challenges**"** ISBN 978-1-84626,2012 International Conference on Security Science and Technology (ICSST 2012).

[16] Shuhua Wu, Yuefei Zhu And Qiong Pu "Cryptanalysis and Enhancements of Three-Party Authenticated Key Exchange Protocol using ECC" JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 27, 1329-1343 (2011)IEEE.

[17] Pierre E. ABI-CHAR, Bachar EL-HASSAN ,Abdallah MHAMED" A Secure Authenticated Key Agreement Protocol Based on Elliptic Curve Cryptography" Third International Symposium on Information Assurance and Security, 0-7695-2876-7/07 2007 IEEE DOI 10.1109/IAS.2007.57.

[18] Zhang JunHong ,Chen XinMeng, Zhu Ping"A Kind of ECC-Homomorphism Key Agreement in Grid" Third International Conference on Semantics, Knowledge and Grid, 0-7695-3007-9/07 2007 IEEE DOI 10.1109/SKG.2007.22

[19] Bin YU , Haiyan LI" Research and Design of one Key Agreement Scheme in Bluetooth" 2008 International Conference on Computer Science and Software Engineering, 978-0-7695-3336-0/08 , 2008 IEEE.DOI 10.1109/CSSE.2008.1263.

[20] Eun-Jun Yoon,Kee-Young Yoo" A Three-Factor Authenticated Key Agreement Scheme for SIP on Elliptic Curves" 2010 Fourth International Conference on Network and System Security, 978-0-7695-4159-4/10 , 2010 IEEE.DOI 0.1109/NSS.2010.101335.

[21] Hongfeng Zhu,Tianhua Liu "A Robust and Efficient Password-authenticated key agreement scheme without verification table Based on elliptic curve cryptosystem" 978-0-7695-4202-7/10 2010 IEEE.DOI 10.1109/CASoN.2010.24.

[22] JIANG Jun, HE Chen "A novel mutual authentication and key agreement protocol based on NTRU cryptography for wireless communications" *J* Zhejiang Univ *SCI 2005 6A(5):399-404* 399

[23] Xuelei Li, Fengtong Wen and Shenjun Cui"A strong password-based remote mutual authentication with key agreement scheme on elliptic curve cryptosystem for portable devices" Appl. Math. Inf. Sci. 6, No. 2, 217-222 (2012) 217.Applied Mathematics & Information Sciences An International Journal.

[24] M. Aydos, B. Sunar, and C. K. Ko.c "An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication" 2nd International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Dallas, Texas, October 30, 1998.

[25] ZHENG Dong , CHEN Kefei and YOU Jinyuan " Multiparty Authentication Services and Key Agreement Protocols with Semi-Trusted Third Party" Vol.17 No.6 J. Comput. Sci. & Technol. Nov. 2002.

[26] Mohsen Sharifi, Saeid Pourroostaei Ardakani, Saeed Sedighian Kashi "SKEW: An Efficient Self Key Establishment Protocol for Wireless Sensor Networks" 978-1-4244-4586-8/09,2009 IEEE.

[27] Rakesh Chandra Gangwar "Secure And Efficient Decentralized Group Key Establishment Protocol For Robust Group Communication" Journal Of Theoretical And Applied Information Technology © 2005 - 2008 JATIT.
[28] Mohammad Sheikh Zefreh, Ali Fanian, Sayyed Mahdi Sajadieh, Mahdi Berenjkoub, Pejman Khadivi "A Distributed Certificate Authority and Key Establishment Protocol for Mobile Ad Hoc Networks" ISBN 978-89-5519-136-3 -1157- Feb. 17-20, 2008 ICACT 2008.
[29] H.-A. Wen, C.-L. Lin and T. Hwang. "Provably secure authenticated key exchange protocols for low power computing clients". Computers & Security, vol. 25, 2006, pp. 106-113.
[30] R. Arshad, N. Ikram" A Novel Mutual Authentication Scheme for Session Initiation Protocol based on Elliptic Curve Cryptography" ISBN 978-89-5519-155-4 705 Feb. 13-16, 2011 ICACT2011.
[31] Simon Blake-Wilsony Don Johnsonz Alfred Menezesx "Key Agreement Protocols and their Security Analysis "the Sixth IMA International Conference on Cryptography and Coding, Cirencester, England, 17-19 December 1997 .
[32] "STANDARDS FOR EFFICIENT CRYPTOGRAPHY "SEC 2: Recommended Elliptic Curve Domain Parameters Certicom Research September 20, 2000
[33] Alfred J. Menezes,Paul C. van Oorschot,Scott A. Vanstone" HANDBOOK of APPLIED CRYPTOGRAPHY" CRC Press, 2nd edition, 1996.
[34] Moncef Amara ,Amar siad "Elliptic Curve Cryptography and its application"7th international workshop on systems ,signal processing and their applications(WOSSPA)IEEE 2011
[35] Fahad Bin Muhaya, Qasem Abu Al-Haija, and Lo'ai Tawalbeh" Applying Hessian Curves in Parallel to improve Elliptic Curve Scalar Multiplication Hardware".International Journal of Security and Its Applications Vol. 4, No. 2, April, 2010.
[36] Sonali U Nimbhorkar, Dr.L.G.Malik" A Survey On Elliptic Curve Cryptography (Ecc)" International Journal of Advanced Studies in Computers, Science and Engineering, vol 1 issue1 ISSN 2278-7917, 5july2012.

AUTHORS PROFILE

Sonali U Nimbhorkar received Post Graduate degree in computer science from RTMNU, Nagpur. She has published more than 17 research papers in various international journals and international conference as an main author and co-author in the field of issues related wireless network ,wireless mesh network, network security and cryptography At present she is assistant Professor in Computer Science & engineering Department in G.H.Raisoni College of Engineering Nagpur, India.

Optical Internet : Possible Attacks on TCP/OBS Networks

K. Muthuraj
Computer Science and Engineering Department
Pondicherry Engineering College
Puducherry, India .

N. Sreenath
Computer Science and Engineering Department
Pondicherry Engineering College
Puducherry, India

***Abstract*— Optical Internet has become the main conduit for all types of virtually sharing communications around the world as it continues its phenomenal growth in traffic volumes and reaches using dedicated optical networks. Optical Burst Switching (OBS) is a technology for Optical Internet to cater the huge bandwidth demands and TCP is the prevailing mechanism to support the Internet. Hence, TCP over OBS has become standard for Optical Internet. There is good amount of research in the area of security in TCP. Also, the issue related to physical network security has been dealt. However, there is limited work is done related to security issues in TCP/OBS networks. Here our work is to identify the possible attacks that may happen in TCP/OBS networks. The NS2 simulator with modified OBS patch is used to identify the same.**

Keywords-OBS Attack; threats on TCP over OBS networks; Optical Internet security; DoS attack on TCP/OBS networks; Orphan burst; Burst tapping attak;Timeout attack; Land attack; Burst header flooding attack; Circulating burst header attack

I. INTRODUCTION

To meet the ever growing demand of bandwidth, copper cables were replaced by fibers in the both the access networks as well as in the backbone networks. Optical fibers not only support huge bandwidth but also have other advantages too such as lower bit-error rate, no interference problem and security advantage without physical damages. Wavelength Division Multiplexing (WDM) technology, is deployed in optical networks, which divides the available bandwidth of the fiber into number of non-overlapping wavelength channels [1]. To carry IP traffic over WDM networks three switching technologies exist namely Optical Circuit Switching (OCS), Optical Packet Switching (OPS) and Optical Burst Switching (OBS). OCS and OPS have their limitations when applied to WDM networks. OCS is not suitable for carrying bursty IP traffic with time-varying bandwidth demand [2-4]. In addition, delays during connection establishment and release increase the latency especially for services with small holding times. OPS, which can adapt to changing traffic demands and requires no reservation, but the optical buffering and signal processing technologies, have not matured enough for possible deployment of OPS in core networks in the future. In this context OBS is the emerging and alternative switching technique, which combines the strengths and avoids the shortcomings of OCS and OPS. Comparison of these switching technologies is given in Table I [5-8].

TABLE I. COMPARISON OF SWITCHING TECHNOLOGIES

Technology	OCS	OPS	OBS
Bandwidth	Low	High	High
Latency	High	Low	Low
Buffering	-	Required	-
Overhead	Low	High	Low
Adaptively	Low	High	High

The rest of this paper is organized as follows. Section II describes the architecture of OBS and about in-band and out-of-band signaling with its functional diagram. The TCP over OBS as explained in Section III. The Section IV shows the main objective of this paper that is the identification of the possible attacks that may happen in TCP/OBS networks in Optical Internet. Finally we conclude and notify the future work in Section V.

II. OBS ARCHITECTURE

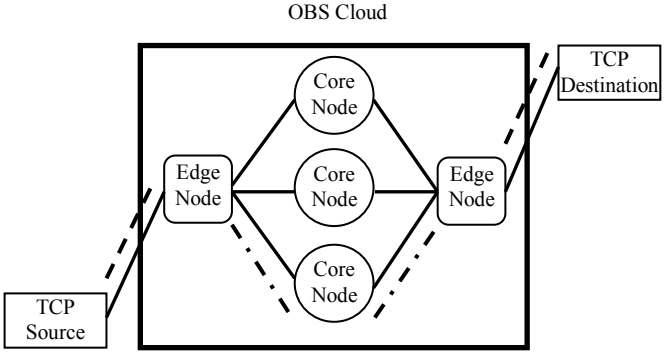


Figure 1. OBS Architecture for Optical Internet

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The pictorial representation of OBS architecture is shown in the above Fig. 1. In general, OBS network is composed of two types of routers, namely edge routers and core routers. Edge routers represent the electronic transit point between the burst-switched backbone and IP routers in an Optical Internet. The assembling of bursts from IP packets and disassembling of burst into IP packets is carried out at these edge routers. Core routers are connected to either edge routers or core routers. It transfers the incoming optical data into an outgoing link in the optical form without conversion of electronic form. In OBS, the basic switching entity is burst which contains the number of encapsulated packets. For every burst there is a corresponding Burst Control Header (BCH) to establish a path from source to destination. BCH of a connection is sent prior to the transmission of Data Burst (DB) with specific offset time on the same wavelength channel is termed as In – band signaling shown in Fig. 2.

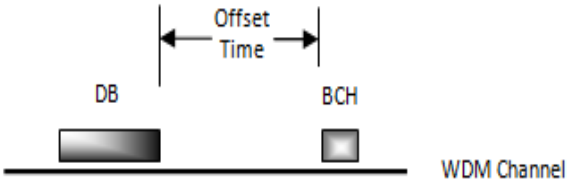


Figure 2. In – band signaling

All BCH's of various connections are sent on the same control channel and their corresponding DBs will sent on the different channels with specific offset time named as out – of – band signaling is shown in Fig. 3.

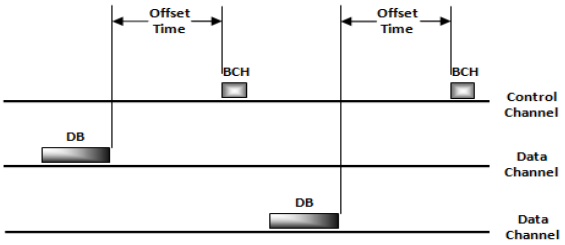


Figure 3. Out – of – band signaling

The Offset time is the transmission time gap between the BCH and DB, which is used to allow the control part in intermediate core nodes to reserve the required resources for the onward transmission of bursts [9 -15].

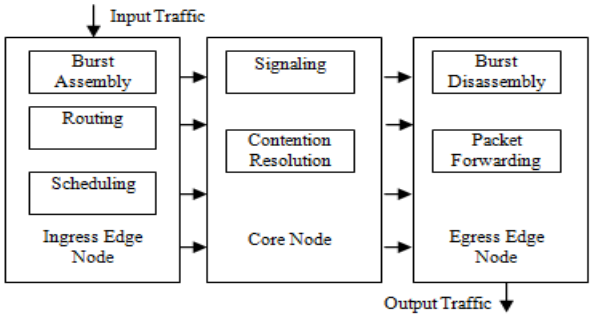


Figure 4. OBS functional diagram

The OBS functional diagram is shown in Fig. 4. It describes the ingress node is responsible for burst assembly, routing, wavelength assignment and scheduling of burst at the edge node. The core node is responsible for signaling and contention resolution. The egress edge node is responsible for disassembling the burst and forwarding the packets to the higher network layer [16 – 22].

III. TCP OVER OBS

In a TCP/IP network, IP layer is involved in routing of packets, congestion control and addressing the nodes. When OBS is introduced in the network, it takes care of routing of data and congestion control. The routing information computed by IP layer need not be considered by OBS routers. It is because, the routes at the OBS are computed based on number of hops and wavelength availability. However, the addressing of the various nodes in the network is not taken care by OBS by default. Hence the functionality of IP may be limited to addressing and packet formation. Due to above reasons, this proposal consider the stack TCP/OBS rather than TCP/IP/OBS. This is shown in Fig. 5 [23 – 29].

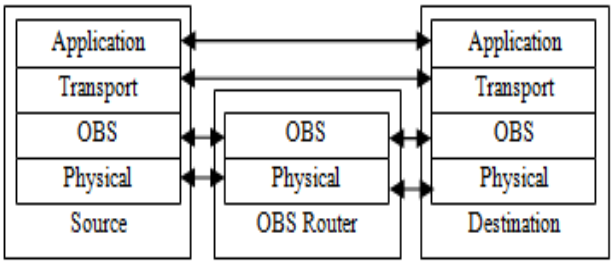


Figure 5. TCP/OBS Layer Architecture

In TCP/OBS networks in Optical Internet there is a degree of possible attacks that may happen, which are explained in the next section.

IV. POSSIBLE ATTACKS IN TCP OVER OBS NETWORKS

The DB that travels over the TCP over OBS network is not secure from the compromised optical nodes. The reason behind that is control signals undergoes O/E/O conversion at every intermediate core node. Every core node requires some time to process the burst header. This makes the burst header vulnerable. There is a possibility of modifying or duplicating the control signal to steal the data burst. Here we describe some of the identified potential attacks and its related work in TCP over OBS network in Optical Internet as follows:

A. Orphan Burst

TCP/OBS network, there is one to one correspondence between the data burst and the burst header, which is sent ahead of the data burst on a separate control channel. The burst header contains the control information and takes care of making the WDM channel reservation for upcoming data burst. It may be possible that any of the OBS core routers rejects the scheduling request for any of the burst header. This will lead to absence of optical path for the upcoming data burst. Since the burst has been launched already, anyway it is going to reach the input of the core router. The burst now cannot be forwarded to

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the next router will become an orphan burst. The orphan burst can able to choose some path unknown in advance. This depends on the configuration of the switching fabric at the time of burst arrival. Since, orphan burst is no longer supported with the core routers it may get tapped off from the communication link by any unwanted party. This will lead to compromising the security of the burst. Fig. 6 shows the example of orphan burst tapped off by an unauthorized party.

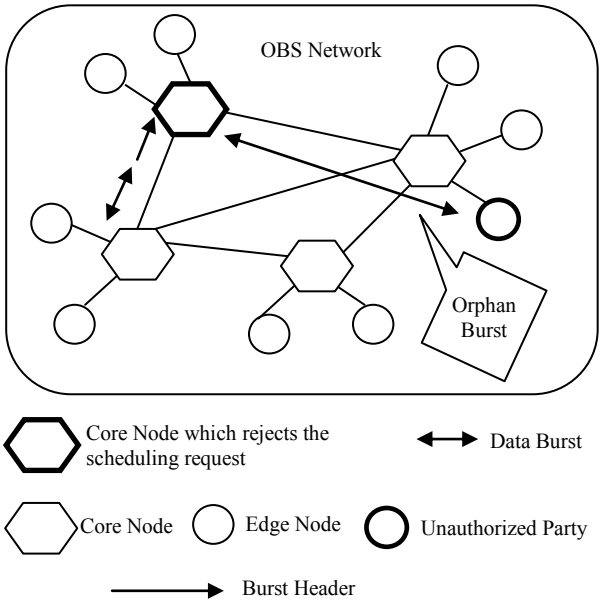


Figure 6. Example of Orphan burst

B. Timeout Attack

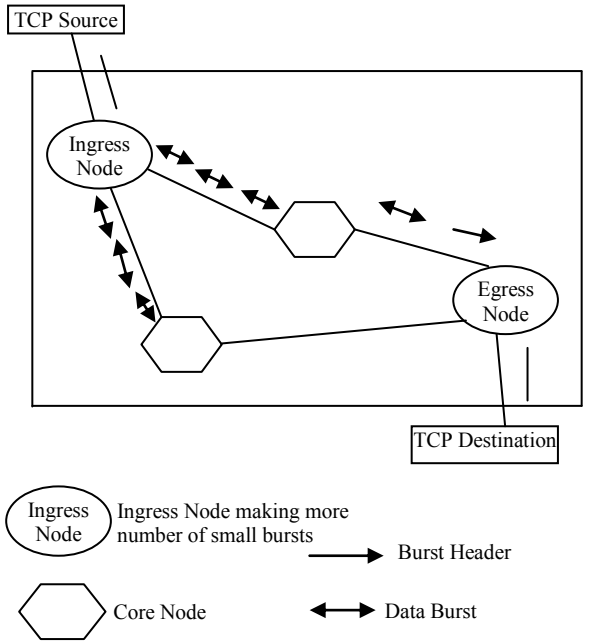


Figure 7. Timeout attack

In ingress router the packets are assembled to form a burst. There are mainly two assembling schemes. First is based on the threshold based and the second is based on the timer-based. In a timer based scheme, a timer is started at the initialization of burst assembly. The latter is based on the maximum number of packets. A data burst is generated when the timer exceeds the burst assembly period or when the maximum number of packets is reached. There is the possibility to change the value of the burst assembly technique at the ingress node. So, if any attacker compromises the Ingress node and using it changes the TIMEOUT value of the nodes to very low. Thus, Ingress node starts to produce the many numbers of small bursts. This will be sent in the communications channel. It will lead to the unwanted traffic shown in Fig. 7.

C. Burst Tapping Attack

To support multicast routing in WDM optical networks, virtual source nodes are unavoidable. An optical node which has both light splitting capabilities as well as the wavelength conversion capability is called as Virtual Source (VS) node. VS node can transmit an incoming burst to multiple destinations on any wavelength. The core node task is to receive the burst header and establish the path for the respective data burst and then forwards it to the next intermediate core node until it reaches the egress node. There is s possibility of making the copy of the burst header and makes it path to reach the attackers destination. To escape from being caught, the compromised node makes the burst header to reach the correct destination. Thus the authenticity of the burst header will be compromised. This attack is named as burst tapping attack as shown in below Fig. 8.

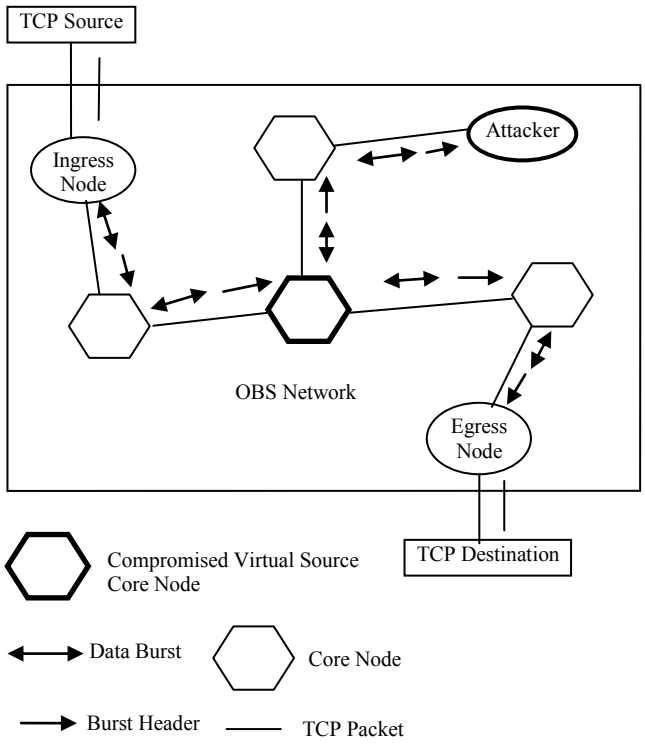


Figure 8. Burst tapping attack

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

D. Land Attack

A virtual Source node can transmit an incoming burst to multiple destinations on any wavelength. In OBS, burst header carries all information about data burst and sent in advance to allocate the resources. In this type of attack the compromised core router maliciously makes a copy of the burst header and modifies its destination address to the source address. So, thus burst header now will change its direction towards the source. This makes the data burst to follow the burst header and reaches source wasting the network resource. Fig. 9. depicts the land attack.

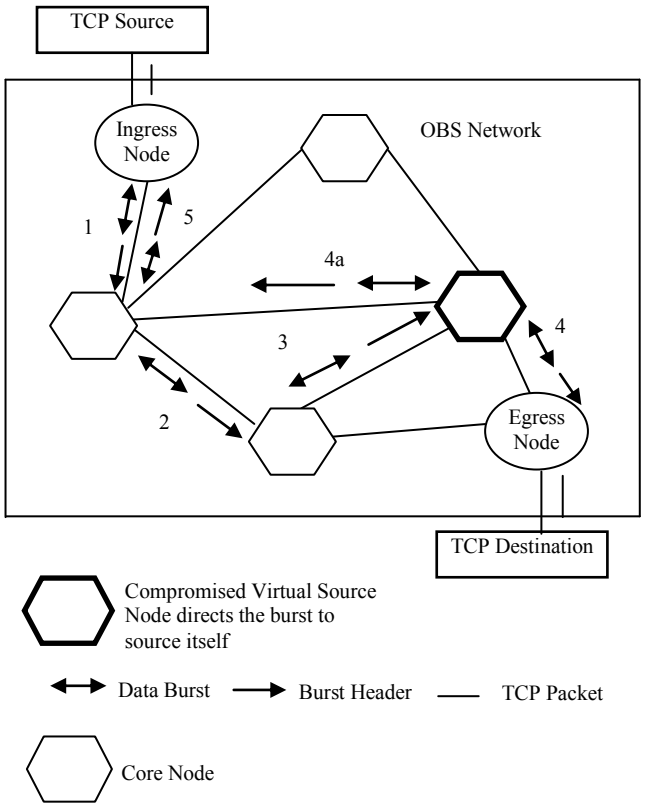


Figure 9. Land attack

E. Burst Header Flooding Attack

Burst header undergoes O/E/O conversion at every intermediate core node. So, it needs some time to be processed at every node. This makes the burst header vulnerable to the attacks. If any optical node is compromised by intruders and using that node, creates multiple copies of the same burst header and advances it to the next node and thereby flooding the next intermediate node with the duplicate copies of the original burst control header. So the next intermediate node tries to make reservations for these fake burst control headers. Hence overflow of buffers will happen at the intermediate core node or if the wavelength conversion is implemented then this bogus burst control header reserves different wavelength for its respective data burst. Thus the uncompromised nodes will not able to reserve the resource if it receives a valid burst header. This attack is called as Burst header flooding attack and it is depicted in Fig. 10.

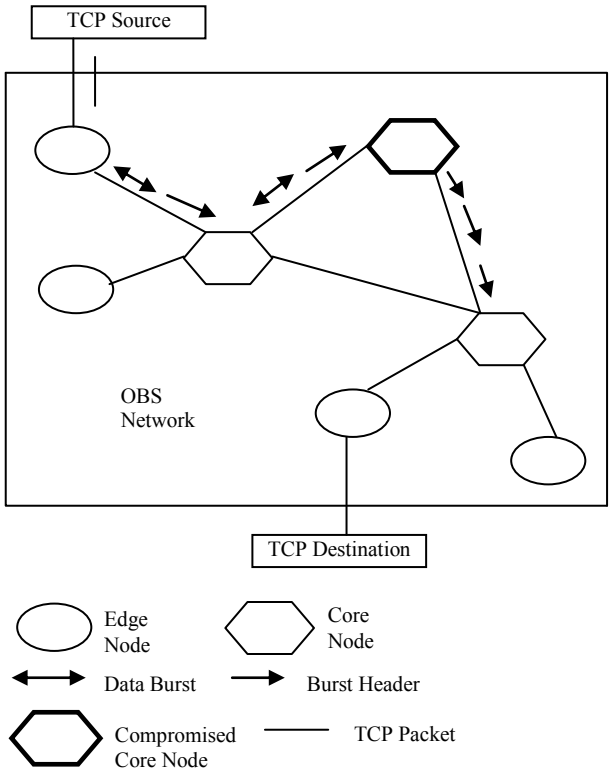


Figure 10. Burst header flooding attack

F. Replay Attack

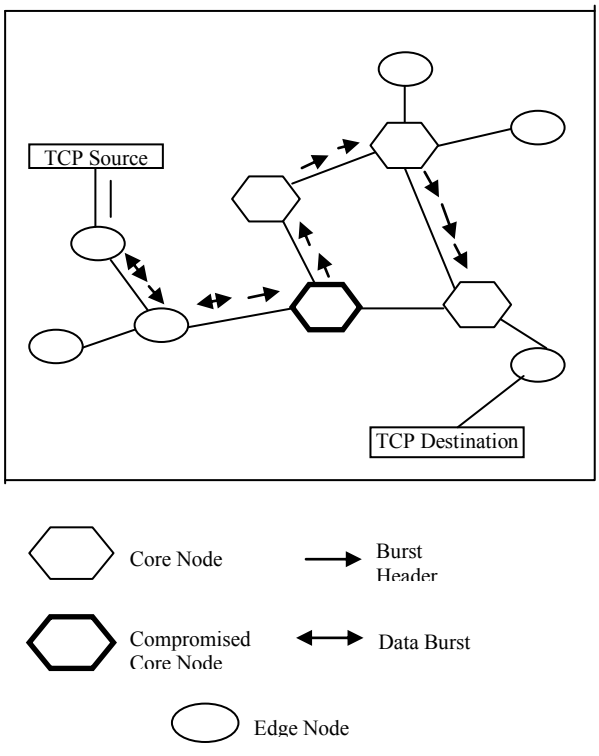


Figure 11. Replay attack

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Burst header sent in advance on the communication channel to reserve the resources for the upcoming data burst. Suppose any of the core nodes rejects the scheduling request, the burst header will be no longer waiting in the nodes. They will get dropped from the communication path. It is the legal burst but the validity of the burst header may ends. It is considered as the legal expired burst. Any attacker takes away the expired burst and makes them inject into the communication channel after sometimes is called as the replay attack. This leads to circulating of the optical burst in the OBS network. It will create the unwanted traffic in the communication channel and thus delivery of the original data burst to the destination will get delayed as shown in above Fig. 11.

G. Circulating Burst Header Attack

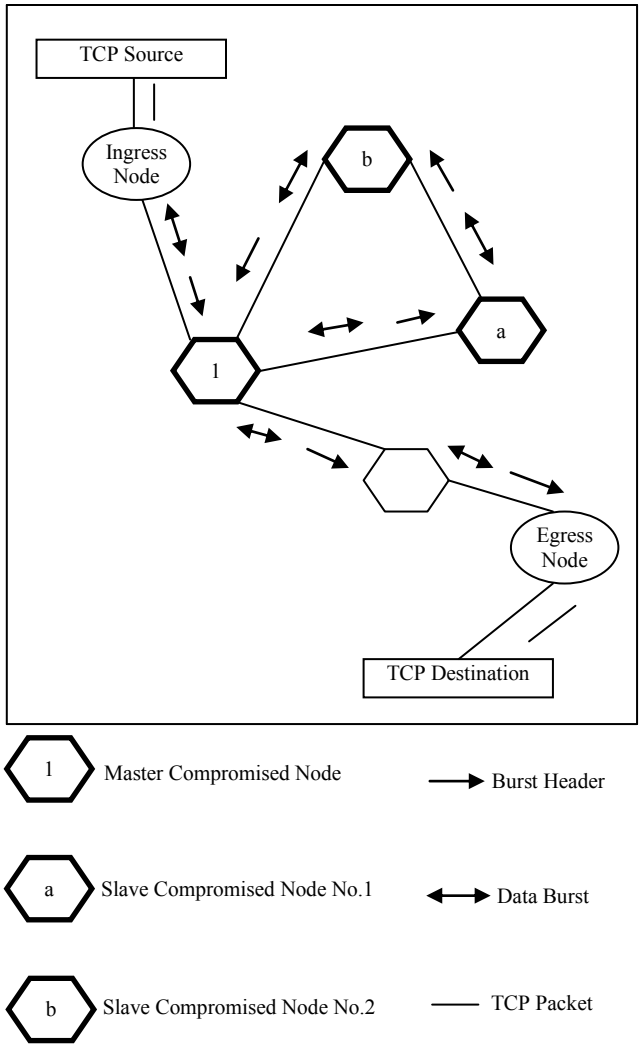


Figure 12. Replay attack

This is one of the attacks which delay the delivery of the data to the destination. In OBS, one or more nodes coordinate and form this type of attacks. One or more compromised core node forms a circuit between them. One of the nodes will act as Master node and others will act as Slave node. Burst header reaching the master node will be circulated among the circuit formed by the compromised nodes for some amount of time. Data burst also will be following the burst header in the channel. After sometimes, the burst header will released from the circuit making its way to the correct destination. This attack will delay the delivery time of the data burst. This attack will also lead to wastage of network resources. Since, circulation of the burst header blocks the resource being utilized by the other new burst header. The above Fig. 12 depicts the circulating burst header attack.

V. CONCLUSION AND FUTURE WORK

In Optical Internet, TCP/OBS networks are the future networks and optical burst switching will turn as the most broadly used technology in the mere future due to its speed and as it provides an end to end optical path among the communicating parties. Since optical burst switching has typical features, it is quite natural to sustain for the security issues. Here we documented the findings of a survey conducted on the security issues on the TCP/OBS networks for Optical Internet. In the future when the optical burst switching is employed in everywhere then some more security threats will arise. Future research in this area will help us to identify and remove other possible attacks in TCP/OBS networks and make optical burst switching technique a superior one for Optical Internet. The countermeasures for the above findings are dealt separately and it will be left out for our future work

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers and the Editor – in – Chief for their valuable comments that have helped us to improve the manuscript.

REFERENCES

[1] B. Mukherjee, " WDM Optical Commutation Networks: Progress and Challenges ", IEEE Journal on Selected Areas in Communications, vol. 18, no. 10, pp. 1810-1823, October 2000.

[2] C. Qiao and M. Yoo, "Optical Burst Switching (OBS) - a New Paradigm for an Optical Internet", *Journal of High Speed Networks*, pp.69-84, January 1999.

[3] S. Verma, H. Chaskar, and R. Ravikanth, "Optical Burst Switching: A Viable Solution for Terabit IP Backbone," *IEEE Network*, pp. 48-53, November/December 2000.

[4] X. Cao, J. Li, Y. Chen, and C. Qiao, "Assembling TCP/IP Packets in Optical Burst Switched Networks., *Proceeding of IEEE Globecom*, December 2002.

[5] X. Yu, C. Qiao, Y. Liu and D. Towsley "Performance Evaluations of TCP Traffic Transmitted over OBS Networks", *Tech. Report* 2003-13, *CSE Department, SUNY Buffalo*, 2003.

[6] Sunil Gowda, Ramakrishna K Shenal, Krishna M Sivalingam and Hakki Candan Cankaya," Performance Evaluation of TCP over Optical Burst – Switched (OBS) WDM Networks", *Proceeding of IEEE ICC,* May 2003.

[7] Arnold Bragg†, Ilia Baldine and Dan Stevenson," A transport layer architectural framework for optical burst switched (OBS) networks", *IEEE communications magazine*, December 2005.

[8] Steven M. Bellovin, A Look Back at "Security Problems in the TCP/IP Protocol Suite", *20th Annual ComputerSecurity Applications Conference (ACSAC)*, December 2004.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[9] Yuhua Chen and Pramode K. Verma," Secure Optical Burst Switching: Framework and Research Directions", *IEEE Communication Magazine*, pp 40-45, August 2008.

[10] B. Harrisa, R. Huntb, "TCP/IP security threats and attack methods", *Elsevier Science Computer Communications vol.22*, pp 885–897. June 1999.

[11] Stamatios V. Kartalopoulos,"Optical Network Security: Counter measures in view of Channel attack", *milcom p.p 1-5, MILCOM*, October – November 2006.

[12] M. Medard, D. Marquis, R. A. Barry and S. G. Finn, "Security Issues in All-Optical Networks", *IEEE Network*, vol. 3, no. 11, pp. 42-48, May/June 1997.

[13] R. Rejeb, I. Pavlosoglou, M. S. Leeson, and R. J. Green, "Securing All-Optical Networks", *ICTON 2003*, vol. 1, pp. 87-90, Warsaw, July 2003.

[14] M. Médard, D. Marquis, and S. R. Chinn, "Attack Detection Methods for All-Optical Networks", *Network and Distributed System Security Symposium, session 3, paper 2, San Diego,* March 11-13, 1998.

[15] Guray Gurel, Onur Alparslan and Ezhan Karasan,"nOBS: an ns2 based simulation tool for performance evaluation of TCP traffic in OBS networks", *European Symposium on Simulation Tools for Research and education in Optical networks, Brest, France*, October 2005.

[16] Vasco N. G. J. Soares, Iúri D. C. Veiga and Joel J. P. C. Rodrigues.,"OBS Simulation Tools: A Comparative Study", *ICC workshop 2008,* pp. 256-260, May 2008.

[17] Oscar Pedrola, Sébastien Rumley, Miroslaw Klinkowski Davide Careglio, Christian Gaumier and Josep Solé-Pareta.,"Flexible Simulators for OBS Network Architectures", *Proceedings of the IEEE ICTON,* June – July 2008.

[18] K. Koduru, "New Contention Resolution Techniques for Optical Burst Switching," *Master's thesis, Louisiana State University*, May 2005.

[19] S. Yoo, S. J. B. Yoo, and B. Mukherjee. All-Optical Packet Switching for Metropolitan Area Networks: Opportunities and Challenges. *IEEE Communications Magazine*, vol. 39, pp. 142-148, March 2001.

[20] Guray Gurel and Ezhan Karasan," Effect of Number of Burst Assemblies on TCP Performance in Optical Burst Switching Networks", *Proceedings of the IEEE BROADNETS 2006,* October 2006

[21] J. Turner, "Terabit Burst Switching," *Journal of High Speed Networks*, vol.8, pp. 3-16, January 1999.

[22] M. Yoo and C. Qiao, "A Novel Switching Paradigm for Buffer-Less WDM Networks," *In Optical Fiber Communication Conference (OFC)*, pp. 177-179, February 1999.

[23] M. Yoo and C. Qiao. Choices, "Features and Issues in Optical Burst Switching (OBS)," *Optical Networking Magazine*, vol. 1(2), pp. 36-44, April 1999.

[24] J. Teng and G. N. Rouskas, "A Comparison of the JIT, JET, and Horizon Wavelength Reservation Schemes on a Single OBS Node," *In Proceedings of the First Workshop on Optical Burst Switching*, October 2003.

[25] B. Lannoo, Jan Cheyns, Erik Van Breusegem, Ann Ackaert, Mario Pickavet, and Piet Demeester, "A Performance Study of Different OBS Scheduler Implementations," *In Proceeding of Symposium IEEE/LEOS Benelux Chapter, Amsterdam*, October 2002.

[26] Pushpendra Kumar Chandra, Ashok Kumar Turuk, and Bibhudatta Sahoo," Survey on Optical Burst Switching in WDM Networks", IEEE, Dec. 2009.

[27] Yuhua Chen, Pramode K. Verma and Subhash Kak.," Embedded security framework for integrated classical and quantum cryptography services in optical burst switching network", Security Comm. Networks 2009.

[28] Sreenath, N., Mohan, G., and Siva Ram Murthy, C.," Virtual Source Based Multicast Routing in WDM Optical Networks", IEEE International Conference on Networks, pp. 385-389, Singapore, September 2000.

[29] Siva Subramanian, P., Muthuraj K.," Threats in Optical Burst Switched Network. Int. J.Comp. Tech. Appl. ", vol. 2, no. 3, pp. 510-514, July 2011.

AUTHORS PROFILE

K. Muthuraj is a Research Scholar and pursuing a Doctoral Degree in Computer science and Engineering at the Department of Computer science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry – 605014, India. He received his B.E in Computer science and Engineering (2000) from Madurai Kamaraj University, Madurai, Tamilnadu, India. He received his M.E in Computer science and Engineering (2008) from Anna University, Chennai, Tamilnadu. His research areas are high speed networks and Optical Internet.

Dr. N. Sreenath is a professor and Head of the Department of Computer science and Engineering at Pondicherry Engineering College, Pillaichavady, Puducherry – 605014, India. He received his B.Tech in Electronics and Communication Engineering (1987) from JNTU College of Engineering, Ananthapur – 515002, Andra Pradesh, India. He received his M.Tech in Computer science and Engineering (1990) from University of Hyderabad, India. He received his Ph.D in Computer science and Engineering (2003) from IIT Madras. His research areas are high speed networks and Optical networks.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A Novel Symmetric Key Distribution Protocol for Data Encryption

S.G.Srikantaswamy
Research Scholar, National Institute of Engineering
Mysore, Karnataka, India
.

Dr.H.D.Phaneendra
Professor & Research Guide
National Institute of Engineering
Mysore, Karnataka, India
.

***Abstract* - Encryption is a mechanism used for protecting data from hackers. The key used for encryption and decryption play a very important role. For conventional encryption both the transmitting and receiving entities use similar key. This key is referred as secret key. Distribution of secret key to communicating entities by a trusted third party is a tedious task. Meet in the middle attack plays a threat to security. In our paper, we have proposed a method to distribute secret key to communicating entities by a trusted third party. The entire process depends on resistance calculation concepts and expressions and equations. Here, by using simple quadratic equations , the key can be distributed to communicating parties without actually transmitting the key itself. Even though the method looks simple, it provides greater security and involves less resources(execution time and memory).**

Keywords - Encryption, Protocol, distribution, Quadratic equation, Authentication, Security

I.INTRODUCTION

Diffie-Hellman key exchange algorithm is used for secure key exchange mechanism. The purpose of the algorithm is to secure exchange of secret key that can be used for subsequent encryption. A new approach to Diffie-Hellman key exchange algorithm has been proposed . The algorithm involves two prime numbers : prime number n and g that is primitive root of n. The paper defines a method to generate private key using equations defined by the communicating entities[1].a new key generation approach has been described which generates a random pool of keys and this key is sent to authorized receiver. During ciphering process the algorithm will select the keys randomly from the pool of keys[2]. Common randomness and secret key generation with a helper has been proposed[3]. Authentic key distribution protocol which employs simple graphical masking method , done by simple ANDing for share generation and reconstruction can be done by simple ORing the qualified set of shares has been discussed[4]. Diffie-Hellman protocol was first proposed in 1976. Diffie-Hellman protocol for key distribution for a group has been discussed in[5]. A three party authentication for key distribution protocol has been proposed [6]. ELK protocol for large-group key distribution has been discussed [7]. A practical solution to the key distribution problem called key predistribution system (KPS) has been suggested in [8]. A method to improve Diffie-Hellman protocol using hash functions has been suggested [9]. An interval-based contributory key agreement approach provides re-keying efficiency for dynamic peer groups [10]. Diffie-Hellman key exchange is a specific method of exchanging cryptographic keys [11]. Key exchange authentication protocol including Diffie-Hellman key agreement , STS protocol ,Encrypted key exchange protocol , shamir's tree-pass protocols have been discussed [12]. Safety measures against man-in-the middle attack in key exchange protocol has been presented [13].Improved key management based on logical key hierarchy is presented[14]. Secret Sharing refers to method for distributing a secret amongst a group of participants, each of whom is allocated a share of the secret. Secret sharing was presented independently by Adi Shamir and George Blakley in 1979 [15]. A key distribution Center (KDC) is part of a cryptosystems intended to reduce the risks inherent in exchanging keys [16]. Needham- Schroeder Distribution and

Kerberos Distributions have been discussed [17].A Multiuser public –key authentication and key agreement Protocol has been proposed [18]. Station-to-Station Protocol, Shamir's three-Pass Protocol COMSET are used for key exchange and mutual authentication[19]. A greater degree of Security can be achieved by maintaining a publicly available dynamic directory of public keys [20].

II.ALGORITHM DESCRIPTION

The proposed algorithm is based on electrical engineering concepts. We know that when two resistances say R1 and R2 are connected in series. Then the total resistance (Rs) of the Series combination is given by **Rs=R1+R2.**

When two resistances R1 and R2 are connected in parallel, the total resistance of the parallel combination(Rp) is given by **Rp = (R1xR2)/(R1+R2).**

Given Rs and Rp, one can calculate R1 and R2 independently as shown below.

Rs= R1+R2

Rp= (R1xR2)/(R1+R2).

Now, R1=Rs-R2

Therefore, Rp= (Rs-R2)x R2/(Rs-R2+R2)

Rp=RsxR2-$R2^2$

$R2^2$-Rs x R2+Rp=0, Thus this is a Quadratic Equation, and given Rs and Rp, R1 and R2 can be calculated by Solving the above Quadratic equation.

Protocol Development and assumptions: Consider Bob and Alice , who are the Communicating entities in this context. Bob and Alice wants to communicate securely by using a Secret Key K.

The Problem here is to distribute key K to Bob and Alice and Solution is being suggested here.

A Trusted third Party [KDC] is considered as an entity to distribute Secret key K to Bob and Alice.

For this purpose, KDC selects two resistance values R1 and R2. And Calculates Rs and Rp.

Rs=R1+R2

Rp=(R1xR2)/(R1+R2)

Let the key K= R1 x R2.

Thus if Bob and Alice knows R1 and R2, they can readily calculate Secret Key K.

Now KDC supplies Rs to Bob and Rp to Alice. Then Bob and Alice Mutual exchanges Rs and Rp using some previously used key.

By Knowing the Values of Rs and Rp, Bob and Alice can determine secret key K , by calculating R1 and R2 and by using the values of R1 and R2, Secret key K can be Calculated as K=R1xR2.

Thus in summary,

Bob and Alice requests for Secret Key to KDC.

KDC sends Rs to Bob and Rp to Alice.

Bob and Alice Mutually exchanges Rs and Rp, and Thus Bob and Alice both posses the values of Rs and Rp.

Bob and Alice independently calculates R1 and R2 by using the values of Rs and Rp, by solving the Quadratic equation.

After determining the values of R1 and R2, Both Bob and Alice independently calculates, Secret key K, by using the relation K=R1xR2.

Thus both Bob and Alice have been Successfully distributed the Secret key K.

III.SYMMETRIC KEY DISTRIBUTION PROTOCOL

Step 1: Bob and Alice sends request for Secret Key K to KDC

Step 2: KDC Sends Rs to Bob and Rp to Alice

Step 3: Bob Sends Rs to Alice and Alice Sends Rp to Bob

Step 4:Bob and Alice calculates R1 and R2 by using Rs and Rp. Then they calculate Secret Key

Key using the relation K=R1xR2.

IV. PROTOCOL ILLUSTRATION WITH NUMERICAL EXAMPLE

Step 1: KDC receives request for Secret key K from Bob and Alice

Step 2: KDC Selects two Values R1=10000 and R2=15000. KDC Calculates Rs and Rp. Rs=R1+R2 and Rp=(R1xR2)/(R1+R2)

Therefore, Rs=10000+15000=25000 and Rp=6000

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

KDC sends 25000 to Bob and 6000 to Alice .

Step 3: Bob Sends 25000 to Alice and Alice sends 6000 to Bob.

Step 4: Bob Calculates the secret Key Value K as follows.

Rs=R1+R2=25000

Rp=(R1xR2)/(R1+R2)=6000

R1=25000-R2

$R2^2$ -25000 R2 +15000=0

R2=10000 and Therefore R1=15000

R2=15000 and Therefore R1=10000

Secret Key K=R1xR2

K=15000x10000

K=150000.

Thus Bob and Alice Successfully calculated the Secret Key Value K and starts communication.

V.STRENGTH OF THE ALGORITHM

It is a very simple approach. Here in this scheme, the secret could be distributed among communicating entities without actually transmitting the key itself. Diffie-Hellman algorithm involves complex modular and exponential operations for key exchange but the proposed scheme involves only simple quadratic equations and hence works fast and consumes less memory.

VI.FEATURES OF THE ALGORITHM

a) Simple and involves simple coding

b) Exchange of Key without transmitting the actual key

c) Provides mutual authentication also.

d) Variable key length based on the values of R1 and R2

VII.CONCLUSION

Many approaches have been used for the purpose of distributing Secret key among communicating entities. These methods are vulnerable to man-in-the-middle attack. Since the key plays the crucial role in the field of cryptography, secure exchange of the key is very important. In the proposed method , we made an effort to exchange secret key between communicating entities based on resistance calculations relations. The method involves Quadratic equation and expressions. The method is effective as it does not involves the transmission of the actual key value between KDC and communicating entities. The Method can be further improved by including modular arithmetic and discrete logarithmic functions.

VIII.REFERENCES

[1] Thanuja. R, Dilip Kumar S-“ A New approach to Diffie-Hellman Key Exchange algorithm”- International Journalof Engineering Research and applications(IJERA)- Vol.1,Issue 3, pp 534-535, 2011.

[2] Naim Ajlouni , asim El-Sheikh and Abdullah Abdali Rashed-“A New Approach in Key eneration and expansion in Rijndael algorithm “-The International Arab Journal of Information Technology, Vol.3, N0.1, January 2006.

[3] Imre Csiszar-‘Common Randomness and Secret Key Generation with a Helper”- IEEE Transactions on Information Theory, Vol.46, No.2, March 2000.

[4] Prabir,Naskar, Hari Narayan Khan, Ayan Chaudhuri and Atal Chaudhuri-“ Ultra Secured and uthentic key Distribution protocol using a Novel Secret Sharing Technique “- international Journal of Computer applications (0975-8887), Volume 19-No.7,April 20115.Vankamamidi.S. Naresh and Nistala V.E.S Murthy-“ Diffie-Hellman Technique Extended to Efficient and Simpler group key Distribution protocol”-International Journal of Computer applications (0975-8887), Volume 4- No.11, August 2011.

[5] Vankamamidi.S.Naresh and Nistala V.E.S. Murthy-“Diffie-Hellman Technique Extendes to efficient and Simpler Group Key Distribution ProtocoInternational Journal of Computer applications(0975-8887),Volume 4- No.11,august 2010.

[6] Suganya Ranganathan , Nagarajan Ramaswamy, Senthil,Balaji, Prabhu, Venkateswaran and Ramesh-“A Three Party Authentication for Key Distribution Protocol Using Classical and quantum cryptography”-International journal of Computer Science Issues, Vol.7, Issue 5, September 2010.

[7] Penrig.A.”ELK, a new Protocol for efficient large-group key distribution “-S&P 2001Proceedings, 2001, IEEE

[8] Proceedings of the International Conference on “ VLSI,Communication&Instrumentation,2011 Proceedings , Published in International Journal of Computer applications (IJCA)

[9] Nan Li-“Research on Diffie-Hellman Key Exchange Protocol”- 978-1-4244-6349, 2010, IEEE

[10] Marimuthu rajaram and Thilagavathy Dorairaj Suresh – “ An interval based contributory key agreement “- International Journal of Network Security, Vol.13, No.2, pp 92-97, sept.2011

[11] http://en.wikipedia.org/Diffie%E2%80%93-Hellman_Key_exchange #Description

[12] Dr.D.S.R.Murthy, B.Madhurarani, G.Sumalatha-“A Study on Asymmetric Key Exchange Authentication Protocols”- International Journal of Engineering and Innovative Technology ,(IJEIT), Volume 2, Issue 2, August 2012

[13] C.Krishna Kumar , G.Jai Arul Jose, C.Sanjeev and C.Suyambulingom-“ Safety Measures gainst Man-in-the middle

attack in key Exchange"-ARPN Journal of Engineering and Applied Sciences, Vol.7, No.2, February 2012.

[14] Nur Alyani Jusoh, Kamaruzzaman, Seman, Norita, M.Norazizi- "The Improvement of Key Management Based on Logical Key Hierarchy by Implementing Diffie-Hellman algorithm "-Journal of Emerging Trends in Computing and Information sciences-Vol.3, No.3, March,2012.

[15] http://en.wikipedia.org/wiki/Secret-Sharing.

[16] http:en.wikipedia.org/wiki/Key_distribution_center

[17] www.ehow.com/info_10043004_symmetric_key_dist
ribution_Methods

[18] A Multi-Party User authentication and Key Agreement Protocol Based on Public Key Cryptosystems-Proceedings of the National Conference on recent trends in Network Security and Cryptography, held at PESIT, Bangalore, Karnataka, India, October 2009

[19] Bruce Schneier -Applied Cryptography-, John wiley & Sons Inc.

[20] William Stallings- Cryptography and Network Security-Third Edition,Pearson Education.

*****

Analysis of Influence of Internet Retail Service Quality (IRSQ) to Consumer Online Shopping Satisfaction at www.kebanaran.com

Imam Tahyudin
Department of Information System
STMIK AMIKOM PURWOKERTO
Purwokerto, Indonesia

Abstract – The purpose of this research was to determine the influence of Internet Retail Service Quality (IRSQ) (website performance, access, security, sensation, and information) to the satisfaction www.kebanaran.com online shoppers. The method of analysis used was path analysis. Based on the research results influence IRSQ variables (performance, access, sensation, and information security), performance variables (X1), access (X2) and sensation (X3) had no significant effect on satisfaction (Y). It showsthat the online shopping website www.kebanaran.com already apply standard terms online stores in general, such as membership, has a return policy, a unique craft product offerings, the choice of language, the choice of currency, the chatroom facility, the product ctalogue about images from different angles and so forth, so that consumers be sure to purchase products through the online shopping website www.kebanaran.com. Security variable (X4) and information (X5) has a significant effect on satisfaction (Y). This shows that security is applied and the importance of information for consumers such as information availability, quality productsinformation, accurate product information is essential so that consumers do not hesitate to deal transaction use online shopping website www.kebanaran.com.

Keyword: Service Quality, Satisfaction, Online Shop

I. INTRODUCTION

There are some experts who defines consumer satisfaction, satisfaction is the level of feelings after comparing the performance or results with the expectations [7]. According to Tse and Wilton, consumer satisfaction or dissatisfaction is the consumer response to the evaluation of the perceived discrepancy between prior expectations and actual performance of the product that is felt after consumption [15]. Wilkie define it as an emotional response to the evaluation of the experience of the product or service consumption [15]. Engel states that satisfaction is an evaluation after purchase as the chosen alternative at least equal or exceed consumer expectations, while dissatisfaction arise if the results do not meet expectations [15]. This suggests that to meet consumers' satisfaction are necessary to identify the consumers' expectations and then realize these expectations, so that consumers feel satisfied.

Among the companies are selling their products online. Higher internet penetration and the growing retail business that markets products and services by online demand the differences measurement of service quality between electronic retail services and the conventional services. Measuring the quality of services is intended to satisfy the consumer.

Quality of services centered on addressing the needs and wants of the consumer and delivery accuracy to offset consumer expectations [14]. According to Janda, Trocchia, and Gwinner [16] conducted research on consumer perceptions of Internet retail service quality and develop measurement scale that examined the quality of services from the perspective of the consumer. Measurement scale is organized into five main dimensions, namely: website performance, access, security of online shopping, shopping sensation, and information. The purpose of this research was to determine the influence of internet retail service quality (performance website, access, security, sensation, and information) to the consumer online shopping satisfaction at www.kebanaran.com.

II. SERVICES QUALITY

The concept of services quality proposed by the Parasuraman et al. are relatively similar to the expectation paradigm which developed in the satisfaction research. In the research by Parasuraman et al measure consumer expectations for service company, these is consumers trust and the perception of reality regarding services received [14].

According Tjiptono stated that quality of services centered on addressing the needs and wants of the consumer and delivery accuracy to offset consumer expectations [14]. So there are two main factors that affect the quality of services, according to Parasuraman, namely expected service and perceived service. If the services received or perceived as expected, the perceived service quality

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

and satisfactory [14]. If the services received exceed consumer expectations, the quality of service perceived as the ideal quality. Conversely, if the services received is lower than what is expected, then the perceived poor quality of services.

According to Zeithaml, consumer expectations for quality of a service is formed by:

a. *Enduring Service Intensifiers*
   This factor is a factor that is stable and encourage consumers to increase their sensitivity to services. This includes expectations caused by others and one's personal philosophy towards services.
b. *Personel Needs*
   One feels the need for fundamental welfare is also very decisive expectations. These needs include the physical, social and psychological.
c. *Transitory Service Intensifiers*
   This factor is a temporary individual factors that increase the sensitivity of consumers to the service, including:
   1) An emergency situation when a consumer really needs the services and wants the company can help.
   2) The consumer consumed the last service can also be a reference to determine the merits of subsequent services.
d. *Perceived Service Alternatives*
   It is the consumer's perception of the level or degree of service other similar companies. If consumers have few alternatives, the hopes for a service tends to be greater.
e. *Self Perceived Service Roles*
   This factor is the consumer's perception of the level or degree of involvement in influencing the services it receives.
f. Situational *Factors*
   This factor consists of all the possibilities that could influence the performance of services which are beyond the control of the service provider.
g. Explicit *Service Promises*
   This factor is the states of organization about their services to consumer. This promise as advertisment, personal selling, comunications with the employee.
h. Implicit *Service Promises*
   Regarding the instructions relating to services that allow consumers about the service and how it should be provided.
i. *Word of Mouth* (rekomendasi/saran dari orang lain)
   Is a statement made by someone other than the organization to consumers. Word of mouth is usually more readily accepted by the consumer, as are those that convey a credible as experts, friends, family and mass media publications.
j. *Past Experience*
   Past experience includes the things they have learned or known consumers from ever received in the past. This consumer expectations evolve over time, as more and more consumers as well as information received increasing numbers of consumer experience [14].

According Wyckof defined service quality is the level of excellence expected and control over the level of excellence to satisfy the consumer [13]. In defining the quality of service, there are some additional characteristics that should be considered. Garvin identified eight dimensions of quality, such as the performance characteristics of the operations on core products, features or additional privileges, compliance with specifications durability, serviceability, aesthetics and perception of quality [13]. However, most of the dimensions are more appropriately applied in manufacturing, therefore modified into seven dimensions that can be applied to service industries such as:

a. Function, the primary performance of the services required
b. Characteristics or additional features, the expected performance or complementary characteristics.
c. Conformance, a decision which is based on the fulfillment of specified conditions.
d. Reliability, belief in services in relation to time.
e. Serviceability, the ability to make repairs if there is some mistake.
f. Aesthetics, consumer experience associated with feelings and senses.
g. Perception, reputation for quality.

According to Janda, Trocchia, and Gwinner conducting research on consumer perceptions of Internet Retail Service Quality and develop measurement scale that examined the services quality from the perspective of the consumer. Measurement scale is organized into five main dimensions: website performance, access, security of online shopping, shopping sensation, and information [16].

III. CUNSOMER SATISFACTION

In the services marketing literature, according to Bolton, Cronin and Taylor described consumer satisfaction as the decision on the basis of a specific service encounter [14]. This is accordance with Oliver'S [14] looked at satisfaction is an emotional reaction that affects attitude. From this perspective, Cronin and Taylor said that consumer satisfaction should confine the service quality and trading decisions specific to long-term attitudes. Consequently cumulative effect of service satisfaction needs to be directed at the evaluation of global service quality frequently [14]. Therefore, the researchers found that satisfaction was preceded

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

by the quality of service [13]. Other researchers found the service quality and consumer satisfaction tested both a global perspective and the specific transaction [13]. According to Oliver and Goose satisfaction evaluation has been linked to the value [14], according to Kasper repeat purchase as well as consumer loyalty to the company [14]. Of course, Fornell in his study of Swedish consumers, which, although quality and consumer satisfaction is important for all companies, so satisfaction is more important than loyalty in the industry such as banking, insurance, postal orders, and transportation.

Many experts who provide a definition of consumer satisfaction. That consumer satisfaction or consumer dissatisfaction is the consumer response to the evaluation of discrepancy or disconfirmation perceived expectations previously (or other performance norms) and perceived actual performance of the product after its use [17].

Consumer satisfaction is an after-purchase evaluation alterantif selected where at least give the result (outcome) equal or exceed consumer expectations, while dissatisfaction arise if the results do not meet consumer expectations or in other words, consumer satisfaction is the behavior of one's feelings after comparing performance (or outcome) that he felt compared to his expectations [17].

Generally, cunsomer expectations are estimates or beliefs about what cunsomers would receive if bought or consuming a product (goods or services). While the perceived performance is the consumer's perception of what he received after consuming the products purchased [17].

According to Janda, Trocchia, and Gwinner conducting research on consumer perceptions of Internet Retail Service Quality and develop measurement scale that examined the quality of services from the perspective of the consumer [16]. Measurement scale is organized into five main dimensions: website performance, access, security of online shopping, shopping sensation, and information.

According to Garvin in evaluating product, service consumers satisfaction generally use multiple factors or dimensions, include [17]:

a. Performance
   That is the principal operating characteristics of the core product being purchased.
b. Features or additional privileges
   That secondary or complementary characteristics
c. Reliability
   That is unlikely to be damaged or fail to use
d. Conformance to specifications
   The extent to which the design and operating characteristics meet predetermined standards.
e. Durability
   With regard to how long the product can continue to be used.
f. Serviceability
   Includes speed, competence, comfort, easy to repair as well as a satisfactory complaint handling.
g. Aesthetics
   Product appeal to the five senses
h. Perceived quality
   That is the image and reputation of the product and the company's responsibility to it.

IV. RESEARCH FINDINGS

A. Path Analysis

To determine the influence of Internet retail service quality (performance website, access, security, sensation, and information) to the consumer online shopping satisfaction at www.kebanaran.com used path analysis. Having tested the validity and reliability of the data and then performed an ordinal transformation of data into interval data by the method of succesive interval (MSI). Once the data is converted into interval data and then do the path analysiscalculation. The results of path analysis calculations can be seen in table 1.

Table1. The results of path analysis calculations

No	Variable	Path coef.	t - count	t -table	Sig.
1	Reality Performance	0,138	1,615	1,9861	0,110
2	Access reality	0,003	0,030	1, 9861	0,976
3	Reality sensation	-0,080	-0,989	1, 9861	0,325
4	Security reality	0,275	3,005	1, 9861	0,003
5	Reality information	0,529	5,927	1, 9861	0,000
Coefficient of determination = 0,564 F Count = 23,757 F table = 2,3134					

Total Influence of proportionally coefficient of determination (R^2) is 0.564, its mean that 56.40 percent of change in satisfaction can be explained by the variation of the variable performance, access, sensation, security and information services. Residual influence apart from the coefficient of determination is 0.4360, meaning that 43.60 percent is explained by other variables not examined.

1. F Test

To examine the path coefficients used F test to describes jointly influence the performance variable (X1), access (X2), sensation (X3), security (X4) and information (X5) satisfaction (Y). From calculating F test obtained F count is 23.757. Using the 95% significance

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

level(α=0,05) and degrees of freedom DF1 = (k-1) = 6-1 = 5, df2 = (n-k) = 98-6 = 92 obtained F table is 2.3134. So F count (23.757)> F table (2.3134) so Ho is rejected. Ho rejection means there is a significant influence of the variable performance, access, sensation, security and information services to satisfaction. The influence showed that the servicesquality provided by the website www.kebanaran.com been in line with expectations and satisfy the consumer.

The image of Ho rejection of F test can be seen in Figure 1.

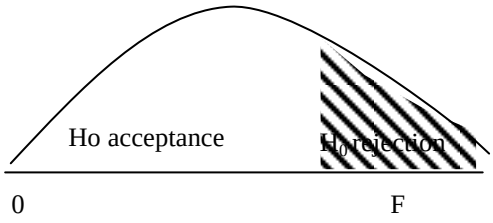


Figure1. Normal curveF test

2. T test

Using the 95% significance level(α = 0,05) and degrees of freedom (n - k = 98-6 = 92) obtained t table is 1.9861, while the result of the calculation result t count performance variable (tYX1) is 1.615. So the t count is less than t table (1.615 <1.9861), which means that the partial performance variable (X1) has no significant impact on satisfaction (Y), so the first hypothesis is rejected. The lack of influence of performance on satisfaction showed that this online shopping website of used tires craft already apply standard provisions, such as the provision of a member willing to transact, have return policies, so that the consumer has no doubt to purchase through the online shopping webisiteat www.kebanaran.com.

tcount access variable (tYX2) is 0.03. So the t count is less than t table (0.003 <1.9861), which means that the partial access variable (X2) has no significant impact on consumer satisfaction (Y), so that the second hypothesis is rejected. The absence of these influenceshowed to date this online shopping website of used tires craft already apply standard provisions, such a unique craft product offerings, the choice of language, the choice of currency and so forth.

tcount sensationvariable (tYX3) is -0.989. So the t count is less than t table (-0.989 <-1.9861), its mean that the partial sensation variable (X3) had no significant impact on consumer satisfaction (Y), so that the third hypothesis is rejected. The absence of such influence because this online shopping website of used tires craft already apply standard provisions as a chatroom facility, product catalogue, so that consumers be convinced to buy used tires craft.

tcount security variable (tYX4) is 3.005. So the t count is greater than the value of t table (3.005> 1.9861), its mean that the partial security variables (X4) has a significant effect on cunsomer satisfaction (Y), so that the fourth hypothesis is accepted. The existence of thisinfuence suggests that security is applied in online shopping website does not make cunsomers hesitate to transact.

Value tcountof informationvariable (tYX5) is 5.927. So the t count is greater than the value of t table (5.927> 1.9861), mean that the partial information variable (X5) has a significant effect on consumer satisfaction (Y), so that the fifth hypothesis is accepted. The existence of thisinfluence suggest that the information presented on the website is very important to convince the consumer to buy the craft used tires product.

V. CONCLUSIONS AND SUGGESTIONS

A. Conclusions

Based on the research revealed that:

1. IRSQ variable (performance, access, sensation, information and security) jointly influentialto consumer online shopping satisfaction at www.kebanaran.com. Its obtained from the results of path analysis, F count (23.757) is greater than the F table (2.3134) so the hypothesis (H1) are received.
2. Performance variables (X1) had no significant influence on satisfaction (Y). This indicates that the craft tires online shopping website already used standard terms online shop in general, such as membership and return policy.
3. Access variable (X2) had no significant effect on satisfaction (Y). The absence of this influence that the craft tires online shopping website already used standard terms online shop in general as a unique craft product offerings, the choice of language and the choice of currency, so that cunsomers are no doubt to purchase

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

through the online shopping website www.kebanaran.com.

4. Sensation Variable (X3) had no significant influence on satisfaction (Y). The absence of thisinfluence shows craft tires online shopping website are standard terms used in general such as the online chatroom facility, the product can diliat images from different angles, so that consumers be sure to buy tires craft through the online shopping website www.kebanaran.com.
5. Security variable (X4) has a significant influence on satisfaction (Y). This shows that the security applied to the website www.kebanaran.com very important so that the consumers not hesitate to transact through the online shopping website.
6. Information variable (X5) has a significant influence on satisfaction (Y). The existence of this influence showed that the importance of information for consumers such as information availability, quality product information, product information is accurate.

B. Suggestions

1. Consumer satisfaction can be enhanced if the operator of the online shopping website further improve the services incorporated in the variables performance, access, sensation, security and information services. These variables should be increased simultaneously in order to optimize consumer satisfaction.
2. To optimize the consumer satisfaction, operator of the online shopping website (used tires craft) can better prioritize attributes incorporated in the performance variables and information. This is because the attributes are incorporated in the variable most dominant influence than other variables.

ACKNOWLEDGMENT

The Authors would like to thank for the support and helpful comments of academicals member of STMIK AMIKOM Purwokerto for this work.

REFERENCES

[1]. Al Rasyid, 1994. Sampling Techniques and Preparation Scale. Program Pasca Sarjana Universitas Padjajaran Bandung.

[2]. Azwar, Saefudin. 2000. Test of Validity and Reliability. Pustaka Pelajar Yogyakarta

[3]. Caruana, Albert.2002. The effects of service quality and the mediating role of consumer satisfaction.*European Journal of Marketing Volume 36 Number 7/8 2002 pp. 811-828.*

[4]. Cooper dan Emory, 1998. Business Research Methods. Erlangga Publisher Jakarta.

[5]. Hazlina Abdul Kadir, Nasim Rahmani and Reza Masinaei. 2011. Impacts of service quality on consumer satisfaction: Study of Online banking and ATM services in Malaysia. International Journal of Trade, Economics and Finance, Vol.2, No.1.

[6]. Jayaraman Munusamy, Shankar Chelliah and Hor Wai Mun. 2010. Service Quality Delivery and Its Impact on Consumer Satisfaction in the Banking Sector in Malaysia. International Journal of Innovation, Management and Technology, Vol. 1, No. 4.

[7]. Kotler, Philip. 2001. Marketing Management (Book 2). Jakarta: Salemba Empat.

[8]. Mowen, J.C. 1995. Consumer Behavior. 4th edition. Prentice Hall Inc New Jersey. Nha Nguyen dan Gaston LeBlanc. 1998. The mediating role of corporate image on consumers' retention decisions: an investigation in financial services.International Journal of Bank Marketing Volume 16 Number 2 1998 pp. 52-65

[9]. Prasetyo Adi. 2008. Influence Analysis Of Service Quality Customer Satisfaction Kaffah BMT Yogyakarta. STAIN Surakarta SEM Institute, Yogyakarta.

[10]. Rambat Lupiyoadi. 2004. Marketing Management Services : Teory and implementation. Jakarta: PT salemba Empat.

[11]. ---------- dan A. Hamdani. 2006. Marketing Management Services. Jakarta: Salemba Empat.

[12]. Sitepu, Nirwana SK. 1994. Path Analysis. Program PascaSarjana Universitas Padjajaran Bandung.

[13]. Tjiptono, Fandy. 1998. Management Services. Andy Publisher Yogyakarta

[14]. ----------. 2000. The principles of Total Quality Service, First Printing, Second Edition, Andi Publisher, Yogyakarta.

[15]. ----------, 2001. Marketing Strategy. Andi Publisher. Yogyakarta.

[16]. ----------, Chandra Yanto, Diana Anastasia. 2003. Marketing Scale. Andi Publisher. Yogyakarta.

[17]. ----------. 2007. Service Marketing. Bayumedia Publishing, Malang.

[18]. Umar, Husein 2000. Conduct Market Research and Marketing. Gramedia Publisher, Pustaka Utama Jakarta.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

AUTHORS PROFILE

Imam Tahyudin was born in Indramayu, West Java, Indonesia, on July 12, 1983. He Received B.Sc. degree from Faculty of Science and Technology, Universitas Jenderal Soedirman Purwokerto, Indonesia in 2006 and M.M. degree from faculty of Economic Universitas Jenderal Soedirman Purwokerto, Indonesia in 2010. He is currently pursuing the M.Eng. degree in the department of Information Engineering, STMIK AMIKOM Yogyakarta, Indonesia, in the field of information system. He is lecturer in the department of information system STMIK AMIKOM Purwokerto, Indonesia. His research interests are in information system management and data mining.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Detecting The Presence Of Hidden Information Using Back Propagation Neural Network Classifier

P.Sujatha
Assistant Professor, School of Computing Sciences,
Vels University,
Chennai, India.

S.Purushothaman
Professor and Dean – PG Studies,
Udaya School of Engineering,
Kanyakumari 629 204,
Tamil Nadu, India.

R.Rajeswari
Research Scholar,
Mother Terasa University,
Kodaikanal, India

***ABSTRACT*:The covert communication based on steganography is a challenging technology for governments. Illegal uses of steganography are Fraud, Gambling, Criminal communications, Hacking, Electronic payments, Harassment, Offenses on Intellectual property, Viruses and Pedophilia. The government needs to find out new techniques to decipher (steganalysis) the information hidden by stegnography. So as to avoid the misusage of steganographic technique, some powerful method is needed to detect the existence of the hidden data in the digital media. This leads to the concept of steganalysis that is a technique of extracting hidden information. This paper uses Artificial Neural Network as a classifier for steganalysis. Back Propagation Neural network algorithm is proposed that uses steepest-descent method to reach a global minimum. However it needs this requires much iteration for the network to converge.**

KEYWORDS:Covert Communication; Steganography; Steganalysis; Artificial Neural Network; Back Propagation Algorithm (BPA)

1.INTRODUCTION

Technological improvement that occurs should improve in an efficient manner to uplift the society. The growth of effective technology gets suppressed by the evolution of security threats. In order to hide information passed by military and Government, steganography is one of the techniques widely used. Steganalysis passes between two phases a) Detection and b) Extraction and that too without knowing the algorithm used for hiding the information. Hence, steganalysis is an art and also a science whereas detection is an art of finding whether hidden message exists or not and Extraction is the science of applying the powerful method to unhide the message.

A .*Classification of Steganalysis*

Apart from all modern sciences and technologies, Artificial Neural Network (ANN) plays a vital role in capturing and representing both linear and non-linear relationships. ANN is an intelligent system which helps to enable machines solves problems like human by extracting and storing the knowledge. To incorporate intelligent method for steganalysis, this paper uses Artificial Neural Network to overcome the drawbacks of the conventional methods. Steganalysis technique can be used for defeating illicit steaganography. It is the method of perceiving the hidden message an extracting it. Steganalysis methods are broadly classified as follows:

1. Supervised learning based steganalysis.
2. Blind identification based steganalysis.
3. Parametric statistical steganalysis.

In supervised learning based steganalysis, a classifier is constructed to differentiate stego and non stego images. Training inputs (both stego and non stego images) will be given to a learning machine. The classification rule is updated by a learning classifier based on prediction and ground truth. Finally, the stego classifier is obtained. This paper focused on supervised learning.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

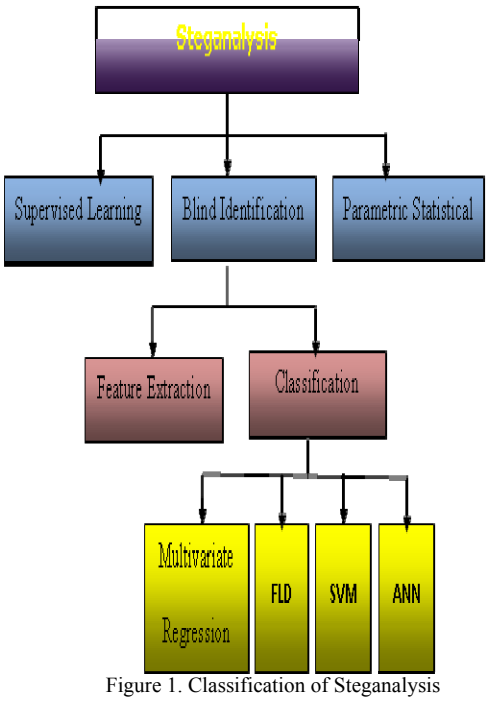


Figure 1. Classification of Steganalysis

In blind identification based steganalysis, the statistical information is used to analyze images. Training data is not available. The specialty of this method is not only used to detect the presence of hidden information but also to extract it. This method includes 2 phases

a.Feature Extraction

b. Classification

a. Feature Extraction: It is a process of creating a set of distinct statistical attributes of an image. These attributes are known as feature. Feature Extraction is nothing but a dimensionality reduction. The extracted features must be sensitive to the embedding artifacts. Image quality metrics, wavelet decompositions, moment of image statistic histograms, markov empirical transition matrix, moment of image statistic from spatial and frequency domain, co-occurrence matrix are some of the feature extraction method.

b. Classification: It is a way of categorizing the images into classes depending on their feature values. Supervised learning is one of the primary classifications in steganalysis. Supervised learning allows learning under some supervision. In this learning, a set of training inputs that includes input features is given as input to train the classifier. After the training, class label is predicted based on the features that are given. Steganalysis use the following classifier.

1. Multivariate regression.
2. FLD.
3. SVM.
4. ANN.

1. Multivariate regression: It consists of regression co-efficients. In the training phase, regression coefficients are predicted using minimum mean square error.

2. FLD: It is a linear combination of features which maximizes the separations. In the classification method, multi dimensional features are projected into a linear space.

3. SVM: This classification method learns from the given sample. It is trained to recognize and assign class labels based on a given set of features.

4. ANN: It is defined as an information processing model that simulates biological neuron system. It includes collection of PE, similar to neuron. Feed forward and back propagation neural networks are commonly used in classification. The classification process has 2 steps, Training and Testing. In a training phase, the Neural Network (NN) associates the outputs with the given input patterns, by modifying the weights of inputs. In a testing phase, the input pattern is identified and the associated output is determined. This paper uses ANN classifier for detecting the presence of hidden information.

In Parametric statistical steganalysis**,** the detection is based on the available statistics. The statistical information may be completely known, partially known, or completely unknown. Hybrid technique combines more than one of the above mentioned methods.

II RELATED WORKS

Supervised learning methods construct a classifier to differentiate between stego and non-stego images using training examples. Supervised learning methods using neural networks as classifiers, gained much importance in recent studies on steganalysis (Liu et al. [9], [10]; Shi et al. [16]; Ryan et al. [15]; Muhanna et al. [13]; Qingzhong et al. [14]) Describing the supervised learning steganalysis method in a general scenario, some image features are first extracted and given as training input to a learning machine. These examples include both stego and non-stego messages. The learning classifier iteratively updates its classification rule based on its prediction and the ground truth. Upon convergence the final stego classifier is obtained. Some of the major advantages using supervised learning based steganalysis are as follows:

1. construction of universal steganalysis detectors using learning techniques and

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

2. Several freely available software packages on the Internet could be directly used to train a steganalysis detector.

Martin et al. [12] found that data hidden certainly caused shifts from the natural set, knowledge of the specific data hiding scheme provides far better detection performance.

A variation of passive steganalysis is active steganalysis, deals in determining or estimating the length of the secret message and the extraction of actual contents of the message (Chandramouli et al. [3]; Fridrich et al. [6]; Chandramouli [4]; Jacob et al. [8]) The methods that estimate the length of secret message or extract the hidden contents are known as embedding-s specific methods. A universal or generic steganalytic method that should be independent of embedding-specific method suits best in digital forensics. Most of the present literature on steganalysis follows either a blind model (Farid [5]; Lyu [11]; Celik et al. [2]) or a parametric model [Harmsen et al. [7]; Tariq et al. [17]). Stating in other terms the present steganalytic work fall broadly into one of two categories: the embedding-specific steganalysis that take advantage of particular algorithmic details of the embedding algorithm, and generic steganalysis that attempts to detect the presence of an embedded message independent of the embedding algorithm and, ideally, the image format. Significant work has been done in detecting steganography using image statistical observations (Zhang et al. [19]; Xiangyang et al. [18]; Anderson et al. [1]). For instance, LSB insertion in raw pixels results in specific changes in the image grayscale histogram, which can be used as the basis for its detection. However, given the ever growing number of steganography tools, embedding-specific approaches are clearly not suitable in order to perform generic and, large-scale steganalysis.

On the other hand, though visually hard to differentiate, the statistical regularities in the natural image as the steganography cover are disturbed by the embedded message. For instance, changing the LSBs of a grayscale image will introduce high frequency artifacts in the cover images. The difference between a clean and a stego image in the high frequency region, presents the artifacts introduced by the embedding. The generic steganalysis detects steganography by capturing such artifacts. A framework for steganalysis based on supervised learning has been designed. The framework was further developed and tested by many researchers. The general framework for generic image steganalysis is followed in the work based on discriminative image features from linear and non-linear classification techniques. Without the knowledge of the embedding algorithm, the proposed work detects steganography.

III METHODOLOGY

In reality, most of the patterns are not linearly separable. Non-linear classifiers are used for pattern classification, in order to achieve good separability. The multilayer ANN is a non-linear classifier, since it uses hidden layer. ANN is used to classify patterns by learning from samples. Different ANN paradigms employ different learning rules. In some way, all these paradigms determine different pattern statistics from a set of training samples. Then, the ANN classifies new patterns on the basis of these statistics.

Various weight updating methods have been developed to learn the patterns by the ANN. They are classified as supervised methods and unsupervised methods. Since both the inputs and outputs are considered, supervised learning technique has been used. The present research work involves modification of existing weight updation algorithm, combination of classical method with ANN to learn more number of patterns, and training the ANN properly for more than two classifications. The performance of the different methods developed has been compared with the performance of BPA, since BPA is a well known algorithm.

The ANN functions on a supervised learning strategy. The inputs of a pattern are presented. The output of the network obtained in the output layer is compared with the desired outputs of a pattern. The difference between the calculated outputs of the ANN and the desired outputs is called the Mean Squared Error (MSE). This error is propagated backwards and the weights between layers are updated. By this process, the MSE of the ANN for the pattern presented is minimized. This procedure has to be adopted for all the training patterns and the MSE of each pattern is summed up. After presenting the last training pattern, the ANN is considered to have learnt all the training patterns through iterations, but the MSE is large. To minimize MSE, the ANN has to be presented with all the training patterns many times. There is no guarantee that the ANN will reach the global minimum; instead, it will reach one of the local minima. The MSE may increase, which means divergence rather than convergence. Sometimes, there may be oscillation between convergence and divergence. Flow-chart for BPA is shown in Figure 2. The training of the ANN can be stopped either by considering MSE or by considering prediction performance as the criterion. When prediction performance is considered as the criterion, test patterns are presented at the end of each iteration.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

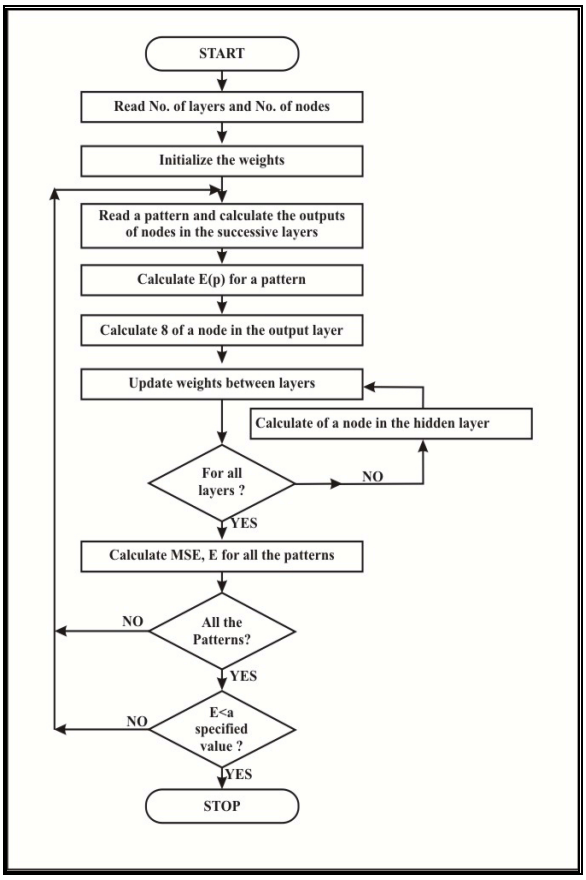


Figure 2. Flow-chart of Back Propagation Algorithm (BPA)

Once the desired performance is obtained, training of the ANN is stopped. When MSE is considered as the criterion, one may not know the exact MSE, to which the ANN has to be trained. If the ANN is trained till it reaches a very low MSE, over-fitting of the ANN occurs. Over-fitting represents the loss of generality of the ANN. That is, the ANN can classify only the patterns, which are used during training, and not the test patterns

B *Implementation Of Back Propagation Algorithm*

The BPA uses the steepest-descent method to reach a global minimum. The number of layers and number of nodes in the hidden layers are decided. The connections between nodes are initialized with random weights. A pattern from the training set is presented in the input layer of the network and the error at the output layer is calculated. The error is propagated backwards towards the input layer and the weights are updated. This procedure is repeated for all the training patterns. This forms one-iteration.

At the end of each iteration, test patterns are presented to ANN, and the prediction performance of ANN is evaluated. Further training of ANN is continued till the desired prediction performance is reached.

FORWARD PROPAGATION

1. The weights of the network are initialized.

2. The inputs and outputs of a pattern are presented to the network.

3. The output of each node in the successive layers is calculated.

$$o(\text{output of a node}) = 1/(1+\exp(\sum w_{ij}x_i))$$

4. The error of a pattern is calculated

$$E(p) = (1/2)\sum(d(p) - o(p))^2$$

REVERSE PROPAGATION

The error for the nodes in the output layer is calculated

$$\delta_{(\text{output layer})} = o(1-o)(d-o)$$

The weights between output layer and hidden layer are updated

$$W(n+1) = W(n) + \eta\ \delta(\text{output layer})\ o(\text{hidden layer})$$

The error for the nodes in the hidden layer is calculated

$$\delta_{(\text{hidden layer})} = o(1-o)\sum\delta_{(\text{output layer})}W_{(\text{updated weights between hidden and output layer})}$$

The weights between hidden and input layer are updated.

$$W(n+1) = W(n) + \eta\ \delta_{(\text{hidden layer})}\ o_{(\text{input layer})}$$

The above steps complete one weight updation. Second pattern is presented and the above steps are followed for the second weight updation. When all the training patterns are presented, a cycle of iteration or epoch is completed. The errors of all the training patterns are calculated and displayed on the monitor as the mean squared error (MSE). E(MSE) = ∑ E(p).

IV. RESULTS AND DISCUSSION

To evaluate the performance of the proposed method, BPA was trained on 1024 images of group 1 (no hidden message), and 512 images of group 3 (with hidden message). Then, patterns from 256 untrained images (Group 4) were calculated and provided as input to BPA for testing. Table 1 presents sample cover images and steganographic images.

Table 1. Images used for steganalysis by BPA

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

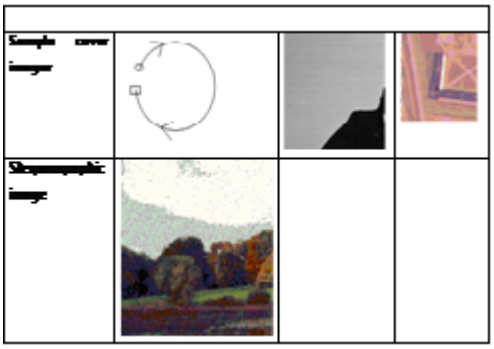


Figure 3 and Figure 4 show intensity values of the patterns used for training ANN. These intensity values correspond to upper nibble of cover images. The maximum intensity value visible is '15' which is equal to '1111'.The number of patterns shown is 7689 in this plot. During training the ANN, two features are used.

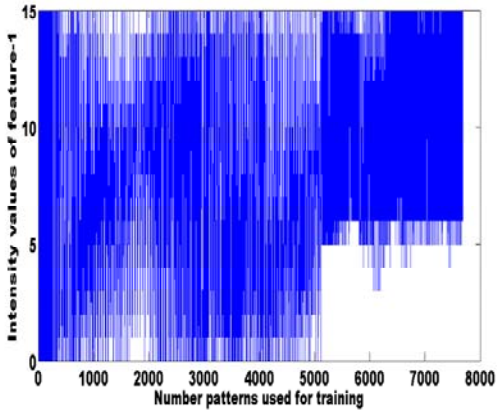


Figure 3. Intensity values of feature-1 of cover image

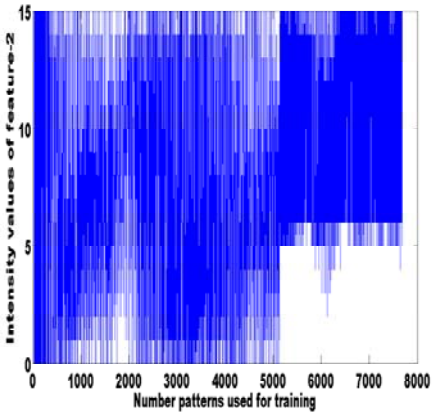


Figure 4. Intensity values of feature-2 of cover image

Figure 5 describes the nature of training took by network. From this Figure, it can be observed that the error reduces drastically from 32 to almost 0 in 2nd iteration, but it still took another 4 iterations to reach required mean square error (MSE).

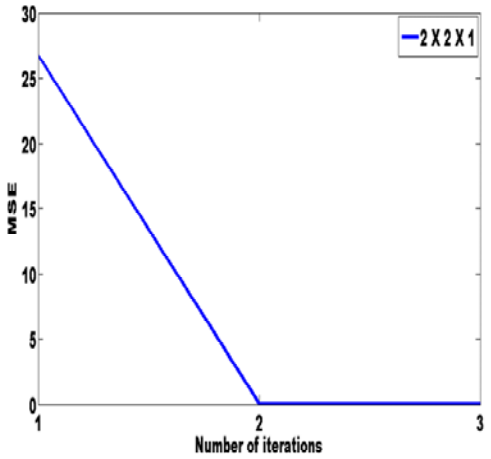


Figure 5 The complexity of BPA during training

In Figure 6, original location of the message refers to the actual information of the image, and detected information tells that the suspect image is a steganographed one. The method produced a positive classification of 94.7% and 5.3% of misclassification. Figure 6 presents the information detected in '□'. The information is detected from the steganographed image presented in Table 1. The 'o' represents the pixels in cover image.

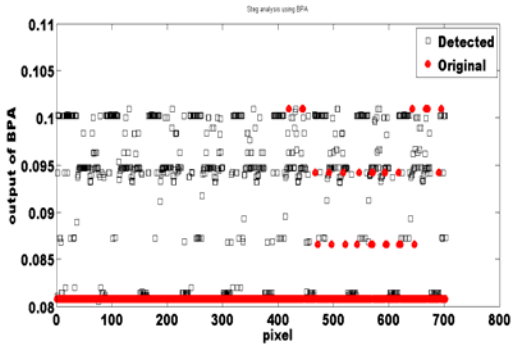


Figure 6. Detection of location of Message by BPA

V CONCLUSION

This paper proposed Back Propagation algorithm which is a supervised learning strategy for steganalysis. The BPA uses the steepest-descent method to reach a global minimum. However when the network is trained with analog data the number of iterations is large for the objective function (J), to reach the desired MSE. The objective function does not reach the desired MSE due to some local minima.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The network converges to one of those local minima or the network diverges. The updating of the weights will not stop, unless every input is outside the significant update region (0.1 to 0.9) and the outputs of the network will be approaching either 0 or 1. This requires much iteration for the network to converge. Hence BPA will produce promising results when it is combined with some other ANN algorithm than using separately.

REFERENCES

[1] Anderson, R., and Goldenstein, S., 2006, Progressive Randomization for Steganalysis, Proceedings of 8th IEEE Workshop on Multimedia Signal Processing, Victoria, BC, pp. 314-319.

[2] Celik, M.U., Sharma, G., and Tekalp, A., 2004, Universal image steganalysis using rate-distortion curves, Proceedings of IST/SPIE's 16th Annual Symposium on Electronic Imaging Science and Technology, San Jose, CA.

[3] Chandramouli, R., and Subbalakshmi, K.P., 2003, Active Steganalysis of Spread Spectrum Image Steganography, Proceedings of International Symposium on Circuits and Systems, ISCAS, Vol. 3, pp. 830-833.

[4] Chandramouli, R., 2003, A mathematical framework for active steganalysis, ACM Multimedia Systems, Vol. 9, No. 3, pp. 303-311.

[5] Farid, H., 2002, Detecting hidden messages using higher-order statistical models, Proceedings of International Conference on Image Processing, New York, pp. 905-908.

[6] Fridrich, J., and Goljan, M., 2003, Digital image steganography using stochastic modulation, Proceedings of IST/SPIE's 15th Annual Symposium on Electronic Imaging Science and Technology, San Jose, CA.

[7] Harmsen, J., and Pearlman, W., 2003, Steganalysis of additive noise modelable information hiding, Proceedings of SPIE Electronic Imaging.

[8] [8] Jacob Jackson, T., Gregg Gunsch, H., Roger Claypoole, L., Jr, and Gary Lamont, B., 2003, Blind Steganography Detection Using a Computational Immune System: A Work in Progress, International Journal of Digital Evidence, Vol. 4, No. 1, pp. 1-19.

[9] Liu Shaohu, I., Yao Hongxun., and Gao Wen., 2003, Neural Network Based Steganalysis in Still Images, IEEE International Conference on Multimedia and Expo, (ICME), Vol. 2, pp. 509 - 512.

[10] Liu Shaohu, I., Yao Hongxun, and Gao Wen, 2004, Steganalysis Based on Wavelet Texture Analysis and Neural Network, Proceedings of the 5th World Congress on Intelligent Control and Automation, China, pp. 4066-4069.

[11] Lyu, S., and Farid, H., 2004, Steganalysis using color wavelet statistics and one-class support vector machines, Proceeding of IST/SPIE's 16th Annual Symposium on Electronic Imaging Science and Technology, San Jose, CA.

[12] Martin, A., Sapiro, G., and Seroussi, G., 2005, Is image steganography natural? , IEEE Transactions on Image Processing, Vol. 14, No. 12, pp. 2040-2050.

[13] Muhanna, M., Turabieh, H., Aljarrah, O., and Elsayad., 2005, A Steganalysis of LSB Encoding in Digital Images Using GLCM and Neural Networks, Proceedings of the 3rd International Conference on Informatics and Systems (INFOS2005), Cairo, Egypt, Vol. 14, pp. 31-37.

[14] Qingzhong Liu, Andrew Sung, H., Jianyun Xu, and Bernardete Ribeiro, M., 2006, Image Complexity and Feature Extraction for Steganalysis of LSB Matching Steganography, 18th International Conference on Pattern Recognition, Vol. 2, pp. 267-270.

[15] Ryan Benton, and Henry Chu, 2005, Soft Computing Approach to Steganalysis of LSB Embedding in Digital Images, Third International Conference on Information Technology: Research and Education, ITRE, pp. 105-109.

[16] Guorong Xuan, Jianjiong Gao, Shi, Y.Q., and Zou, D., 2005, Image Steganalysis Based on Statistical Image Moments of Wavelet Subband Histograms in DFT Domain, IEEE 7th International Workshop on Multimedia Signal Processing, Shanghai, China, pp.1-4.

[17] Tariq Al Hawi, Mahmoud Al Qutayri, and Barada Hassan, 2004, Steganalysis attacks on stego-images using stego-signatures and statistical image properties, IEEE International Conference on Analog and Digital Techniques in Electrical Engineering, Thailand, Vol. 2, pp. 104-107.

[18] Xiangyang Luo, Bin Liu, and Fenlin Liu, 2005, Detecting LSB Steganography Based on Dynamic Masks, Proceedings of 5th International Conference on Intelligent Systems Design and Applications (ISDA'05), pp. 251-255.

[19] Zhang, T., and Ping, X., 2003, A new approach to reliable detection of LSB steganography in natural images, Signal Processing, Science Direct, Vol. 83, No. 10, pp. 2085-2093.

[20] Shaohui Liu, Lin Ma, Hongxun Yao, and Debin Zhao, 2009, Universal Steganalysis Based on Statistical Models Using Reorganization of Block-based DCT Coefficients, 5th International Conference on Information Assurance and Security, Vol. 1, pp. 778-781.

[21] Sheikhan, M., Moin, M.S., and Pezhmanpour, M., 2010, Blind image steganalysis via joint co-occurrence matrix and statistical moments of contourlet transform, 10th International Conference on Intelligent Systems Design and Applications (ISDA), pp. 368-372.

[22] Zhi-Min He, Ng, W.W.Y., Chan, P.P.K., Yeung, D.S., 2011, Blind steganalysis with high generalization capability for different image databases using L-GEM, International Conference on Machine Learning and Cybernetics (ICMLC), Vol. 4, pp. 1690-1695.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

A Discrete Event Simulation Approach on Polarized based Quantum Key Distribution Protocols using OptiSystem™

Abudhahir Buhari, Zuriati Ahmad Zukarnain, Shamla K.Subramaniam
FSKTM
University Putra Malaysia
Serdang, Malaysia

Hishamuddin Zainuddin
INSPEM
University Putra Malaysia
Serdang, Malaysia

Suhairi Saharudin
MIMOS BERHAD
Technology Park Malaysia
KL, Malaysia

Abstract— **In this paper, we present a discrete event approach to simulate the various quantum cryptographic protocols based on commercial photonic simulator OptiSystem. We modeled and simulated polarization based and decoy state based quantum key distribution protocols. We applied same experimental setup procedure and parameters on simulation models with slight modification on few photonic components. Probabilistic mechanism is applied in the entire events which satisfy the quantum spirit. Further, we have also modeled some eavesdropping attacks and free space quantum key distribution. Similarity score is high on our simulation result compare with experimental results. Finally, we packaged the simulation concept as an additional library to the simulator. The usability, modularity, reliability and robustness are the main core concern of our proposed simulation library.**

Keywords - quantum cryptography; quantum key distribution; discrete event simulation, qkd-optisystem simulation

I. INTRODUCTION

Quantum Key Distribution (QKD) is a promising technology to achieve secure key distribution. As it is based on the laws of quantum mechanics, it cannot be bounded by the computational limit. Moreover, QKD can produce unconditional security, which is the deficit in digital cryptography. Further, QKD is the mature field of quantum cryptography and available in the markets. However, QKD still requires more development to achieve the heights like digital cryptography.

QKD can be done by various techniques. Faint-laser and entanglement based are prominent in theoretically and experimentally. Faint-laser or weak coherent laser is slightly edger than entanglement based techniques in terms of practical feasibility. Polarization encoding is a traditional encoding technique used in QKD experiments, i.e. BB84 [1], B92 [2], SARG04 [3], six-state [4, 5], decoy state [6] and free space QKD [7-9]. Other encoding i.e. phase and amplitude are the contemporary tactics. Nevertheless, polarization encoding is still a dominant technique in both fiber-optic and free-space. Fig. 1 depicts an overview of QKD hardware architecture.

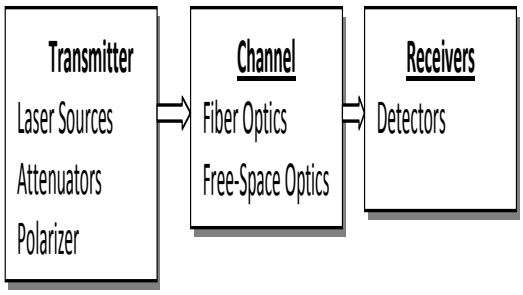


Figure 1. An overview of QKD major experimental components

Photon is mainly used as qubit in QKD experiment. By utilizing the polarization property of a photon which is emitted and attenuated by laser source and attenuator, encoding the information is simple. Using the various polarizer with different angle, information can be encoded compactly to transmit. Further, the non-cloning theorem and Heisenberg property are directly applied to the photon polarization state to detect the eavesdropper. Hence, polarization plays a significant role in QKD architecture. On the other hand, polarization state is vulnerable to various factors, which results questioning in the robustness of QKD, i.e. imperfect devices, noises, channel-losses and detector deficiencies.

Mathematical proofs and numerical simulation based researches are dominant in quantum cryptography area. Nevertheless, the overlook on hardware impact has reduced the accuracy of the results. This is the fact that QC is a combination of hardware and technique. Moreover, QKD lacks of the commercial or free based performance analysis simulator for computer network or digital cryptography protocols. The results from the simulator are de facto standard and required prior to implementation. Unlike, QKD researches to have a gap between theoretical and experimental work and can be filled by efficient simulation only. In this paper, we designed and presented a discrete event simulation approach to evaluate performance analysis of QKD protocols using OptiSystemTM.

OptiSystem is a commercial photonic simulator which is widely used in telecommunication. The systematic approach and experimental QKD equivalent setting and efficient usage of components of the simulator culminate at effective

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

performance analysis on QKD protocol especially in hardware components. We applied discrete event simulation technique which able to observe and understand each stage of the simulation clearly.

This work is an extent of our previous work [10]. To make this paper as a full content, we described elaborately on the simulation approach. In proposed simulations, we modeled transmitter and channel modules equivalent to experimental QKD setup with slight modification. However, receiver module still lacks of implementation of the practical detector. Instead of the detector, we have used an intrinsic simulator's components i.e. visualize the library. Further, we developed the simulation models as an additional library and we elaborate as software quality requirements in the following table.

TABLE I. ANALYSIS OF OPTISYSTEM SIMULATION AS SOFTWARE QUALITY REQUIREMENTS

Quality	Impact	Descriptions
Reliability	High	The setting of each component can be configured and changeable. The results of the simulation model can be compared with QKD experimental results for optimization.
Robustness	High	Simulator does not accept faulty links and illogical settings. Each event can be monitored by the visualize component.
Usability	High	Simulation models look like collection of connected graphical icons. Users can simply drag and drop components to develop the model. Simulation model run by simple button press and all the background mechanism are displayed during compilation. Report is generated by manual action or simple script coding. Further, graphs and other images are exportable to convenient format.
Portability	Medium	Simulation model can be copied or moved as a file and run on the other machines which contains OptiSystem. However, OptiSystem is required a commercial licesnce.
Maintain-ability	Low	Maintainability is basically low in even the proc'ess of optimization and customization. This is due to the factor that changes are simple to make.
Efficiency/ Performance	High	Fundamentally, OptiSystem contains most of the photonic components used in the telecommunications. But, some QKD related components are not directly available. Performance analysis of the simulation model is extracted into visualition graphical mode, graph and data. Further, the simulator has diverse graphs, data export to Matlab & Excel, import data from the file and able to create subcomponent from the simulation model and using Matlab. Simulation can be run by user defined number with less memory consumptions.

II. METHODOLOGY

In our previous work [10], BB84 with Eve's attacks and noise immune QKD [11] are simulated. Optisystem [12] provides drag and drop approach to build the models. Further, VBScript and Matlab extension are available to build from the user defined program. In this paper, we consider other QKD schemes i.e. B92, six-state protocol, decoy-state protocol and free-space QKD are simulated. A short description on QKD schemes is presented. For the detailed version, please refer to the particular QKD protocols' references.

We designed the simulation models as same as telecommunication modeling scenario. According to the scenario, we classified simulation models into three modules namely transmitter, channel and receiver. In this paper, both transmitter and channel modules similar to the experimental QKD setup with slight modification on some photonic components. The receiver is lacking of implementation of experimental detectors. Thus, receiver module is weaker simulation in compare with other two modules. The following subsections explain the modules briefly.

A. Transmitter Module

Optical Source: OptiSystem provides wide variety of transmitter components for QKD. Most of the components and its features are correlated with experimental QKD setup components. Broad range of components available for optical source laser like coherent wave (CW), light-emitting diode (LED) , pump laser, vertical-cavity surface emitting laser (VSCEL) and its variants, i.e. spatial and laser rate.

Passive Optical Components: Under the "passive library/optical" section, several components available ranges from attenuators, polarization, power combiners, isolators, couplers, circulator, power splitters and delay.

From the "Tools library," we have used fork, select and switch components. Particularly, we swapped experimental QKD vital component called the polarization beam splitter (PBS) with select and switch component. The role of select component is to choose one signal from many signals. Contrast to 'select', 'switch' chooses one of many outputs from one input. On other hand, component 'fork' play duplication of signal. This is used for customization of simulation.

B. Channel

Under the "optical fibers" library, single mode and multimode fibers are available. Simulator also provides intrinsic characteristics like dispersion; polarization mode dispersion (PMD) and noise's parameters can be set.

C. Receiver

The vital component of receivers like photo detectors PIN and APD are provided in the simulator, but we have a synchronize problem with our proposed simulation models. Therefore, we have employed other inbuilt components; i.e. optical spectrum analyzer, polarization analyzer, polarization meter and optical time domain visualize under the "Visualizer" library. Thus, these components are covering the receiver

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

module of our simulation models. However, this set up has a huge impact on the quantum bit error rate (QBER) and acts as an ideal detector.

D. Simulation Setup

We conduct two sets of experiments on each protocol. First set contains 10000 iterations while second set contains 25000. The results obtained from the simulation models has the standard channel length is 100km for both fiber-optic and free-space QKD. The data are exported to excel worksheet by a small vbscript code for further calculations. We tested all simulation models with and without noiseless channel, eavesdropping attack for QBER calculations. In all simulation models, detector in the receiver module considered as a perfect device.

III. QKD Protocols Simulation Models

A. BB84 Protocol with Eve Attacks

BB84 protocol is a visionary protocol which leads active researches on possibilities of quantum cryptography (QC) for last three decades. BB84 is a two-party quantum key distribution system. Conveniently, two parties called Alice and Bob are legitimate users while Eve is adversary or illegitimate user. In BB84, Alice chooses a random bit and encoded in any of four polarization states namely horizontal (0°), vertical (90°), left (-45°) and right (45°). Both horizontal and right represents bit 1 and remaining angles represent bit 0. On the other side, Bob randomly chooses one of two conjugate bases (0/90 or 45/-45) to measure the incoming qubit. If he chooses correct base, corresponding detector would click. For the wrong bases, no click or two-clicks would be triggered. Both Alice and Bob note down all the bases and timing. During the post-quantum discussion, wrong bits will discard. Both calculate quantum bit error ratio. If the value greater than standard, they continue with further actions of the key-distillation process. After sifting and privacy amplification techniques, both Alice and Bob established shared secret key.

In QC protocols, random selection of bases acts like the critical role, to achieve randomness in our simulation models. We utilized simulator's inbuilt functions and tested the results with the NIST test suite [13]. The results passed the frequency test. Now let see the simulation setup for BB84. In Fig. 2, we applied four CW source, four attenuator (0.1 attenuation to attain single photon) and four polarizer. The component 'select' act as polarization beam splitter and configured to choose randomly one of four polarization states on each iteration. On Bob's side, we designed the detector in a way to randomly choose to allow the signal or not. If detector shows signal strokes assumed right polarization base else wrong base. In our simulation, Eve has the variety of attacks on incoming qubit. We designed the Eve's capabilities as she can allow the incoming qubit, or modify the incoming qubit ,or generates new qubit or null qubit. These ideas are based on standard eavesdropping techniques found in the literature [14-16]. Generally; they classified Eve's attack as general attack, collective attacks and coherent attack. Recently, more sophisticated attacks have been presented. Further, OptiSystem supports to create subsystem from the models.

We created a new subsystem from the Eve's module. This subsystem can be attached to other models without creating again.

B. B92 Simulation Model

B92 is a lighter version of BB84. This protocol uses only two states of polarization. The setup requirement is similar to the BB84 setup. In the receiver side, receiver needs to choose between one polarizer. Here, we implemented optical null as differentiation of polarizer. Optical null is equivalent to wrong polarizer. Fig. 3 depicts the simulation model.

C. Six-state Simulation Model

Fig. 4 represents six-state protocol, which applies three conjugate bases for the encoding, but it otherwise identical to the BB84 protocol. The probability for Alice and Bob choosing compatible bases is only 1/3. In our simulation setup, polarization rotator has used to cope with the sixth state. Receiver module is modified in a way each visualizer able to show the right polarization in case of correct base. This is done with help of polarization rotator component.

D. Decoy-state Simulation Model

SARG04 protocol differs only in the BB84 key-distillation process. The simulation model which we develop can be applicable to both BB84-decoy state and SARG04-decoy state.

In this simulation, we implement one-decoy state mechanism. The decoy state is created by simple changes in the intensity of the photon using attenuator. We set 80% signal state and 20% of decoy state in the select option. To identify the decoy state and signal state in the receiver side, we utilized optical power meter. In this simulation, attenuation value set for signal state is 0.1 and for decoy state is 0.8. This model is shown in Fig. 5.

E. Free-space Simulation Model

Free-space QKD implementation is simple. OptiSystem has got the free-space library in which free space optics (FSO) component available. FSO contains two satellites (both sender and receiver), and configuration settings are presented in the Fig. 6. On the receiver side has small modification, and it comprises two polarization rotators. Each polarization rotator is set with different angle. The result can be viewed in the polarization analyzer.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

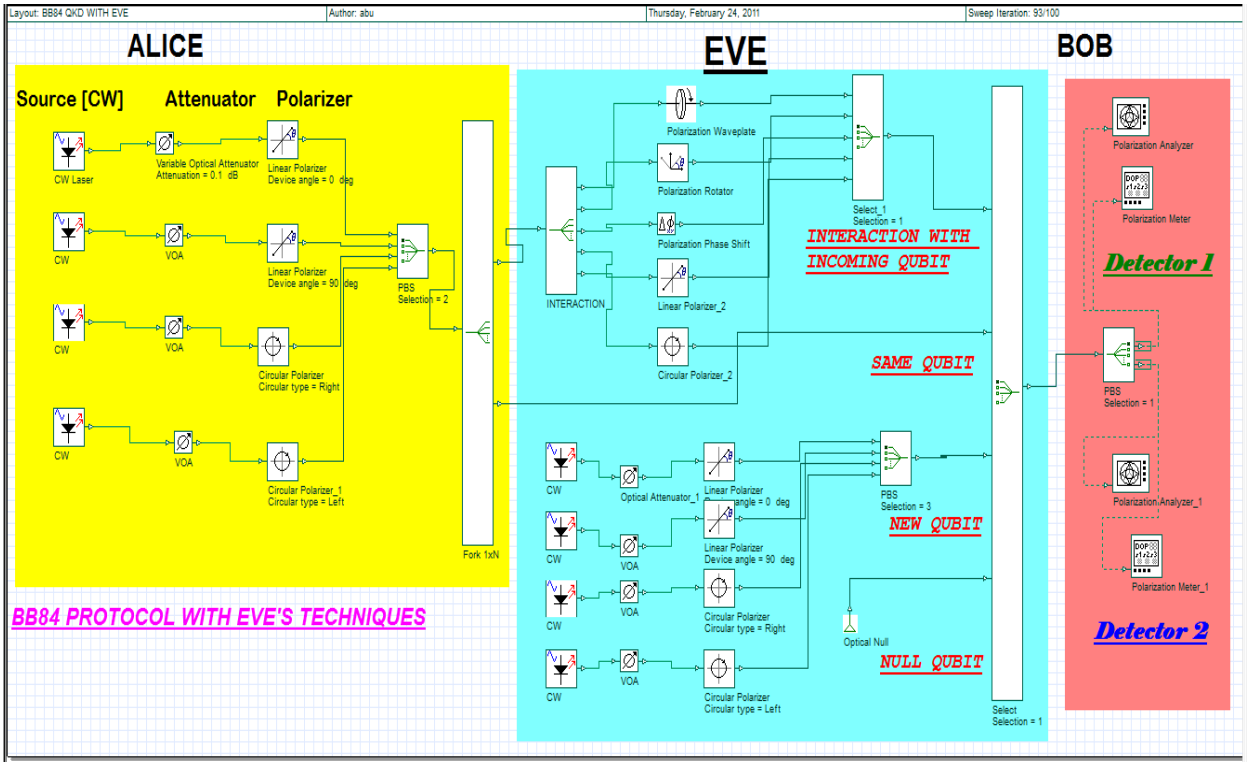


Figure 2. BB84 with Eve's Attacks.

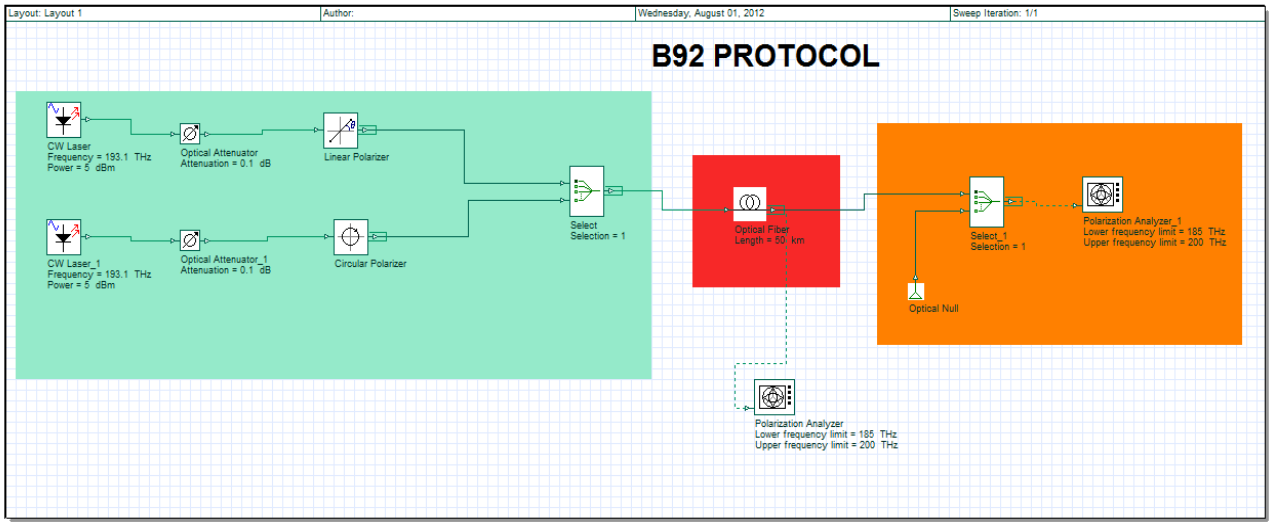


Figure 3. B92 simulation model.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

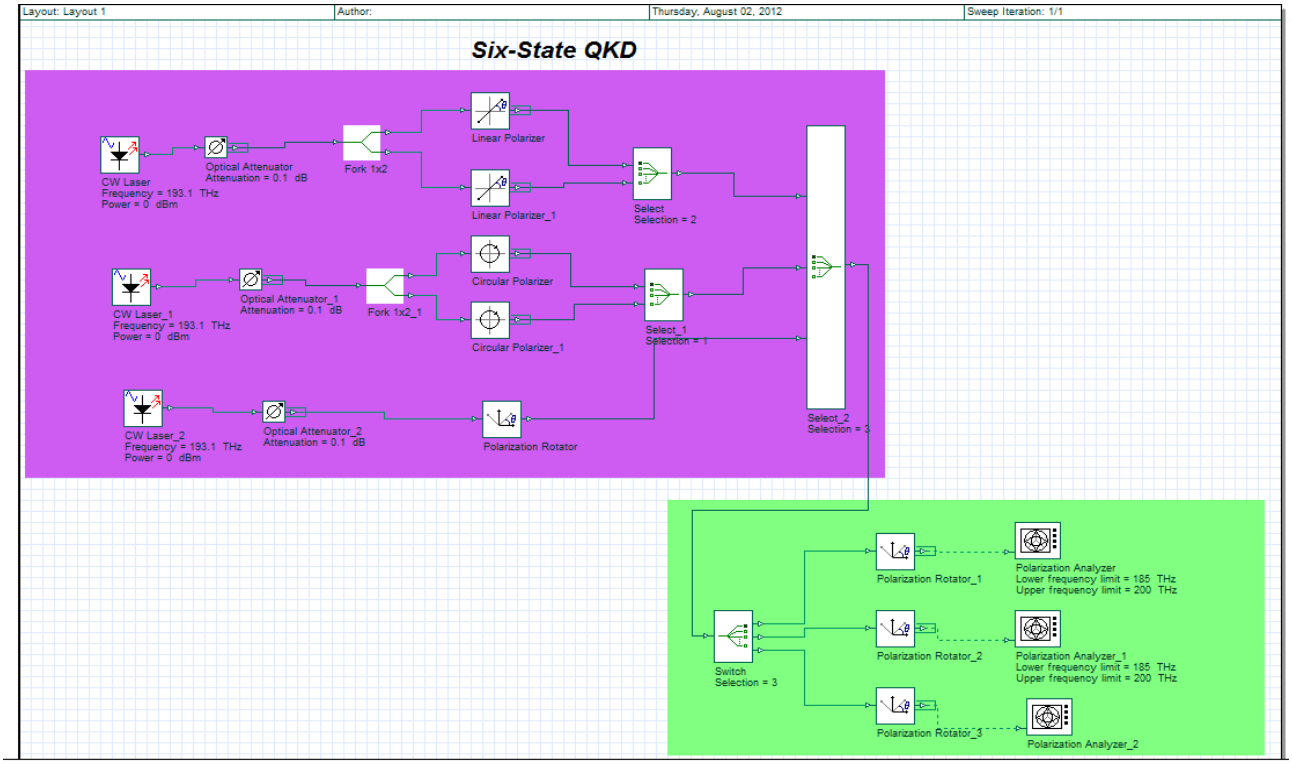


Figure 4. Six-state QKD simulation model.

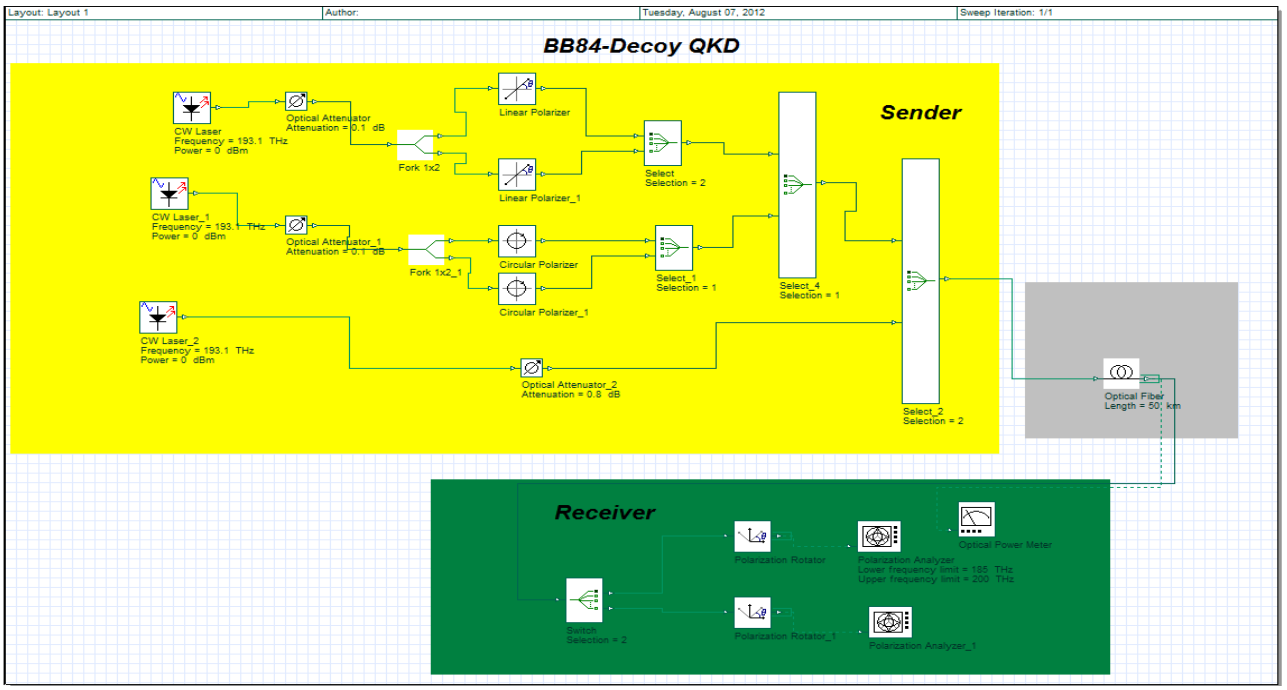


Figure 5. BB84-Decoy state QKD simulation model.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

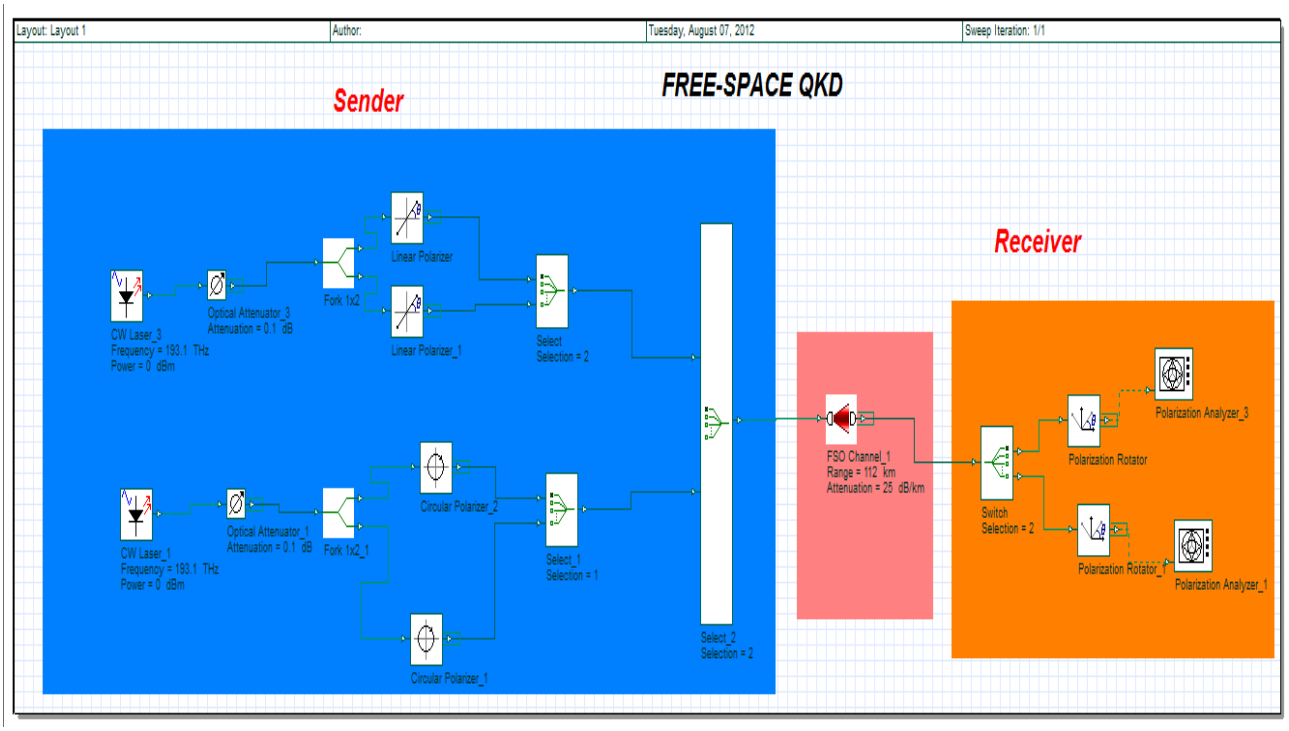


Figure 6. Free-space QKD simulation model.

IV. Results and Discussion

The overall results of the simulation are better than the experimental QKD is due to two main factors. First reason is inclusion the single photon source, and the second one is the omission of detector's issues. The experimental QKD detector suffers issues like dark count, low efficiency and there is a no longer available device to produce the single photon. Normally, in QKD experiment, fain-laser is used with high attenuation to produce photons or qubits. Further, emission of photons is based on Poisson distribution. This distribution suffers photon-number splitting (PNS) attacks. Thus, the omission of these factors increases the QBER rate in the simulation results.

Fig. 7 depicts the simulation results of protocol in an ideal channel and ideal detector settings. Here ideal refers to noiseless and errorless. Further, except BB84-Eve protocol all other protocols simulated without eavesdropping technique. Thus, the results are higher to the experimental QKD results. BB84-Eve shows lowest QBER rate while B92 and Free-space show 50% QBER rate. BB84-decoy state protocol shows around 40% QBER; this is due to the combination of signal state and decoy state detection. Finally, six-state shows 42% QBER.

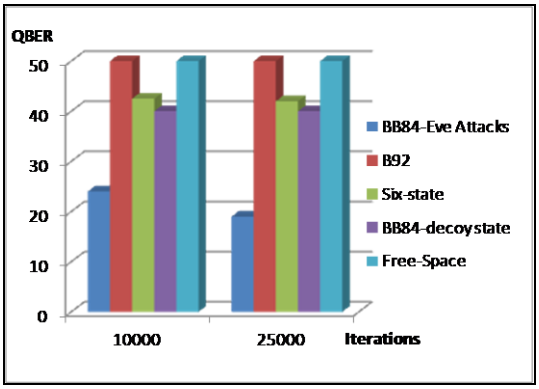


Figure 7. Ideal channel and ideal receiver

Fig. 8 represents the simulation results of protocol with noise channel and ideal detector. As expected the QBER rates decrease. The interesting result is BB84-Eve with 12% for iteration set II. This is lower than standard QBER rate. It seems probabilities of Eve's attack and transmission loss is high. Other protocols to suffer a marginal decrease around 5% while free space QKD suffers 10% drop in the QBER rate. This is due to inclusion of geometrical loss, propagation delay, beam divergence receiver loss and transmitter loss.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

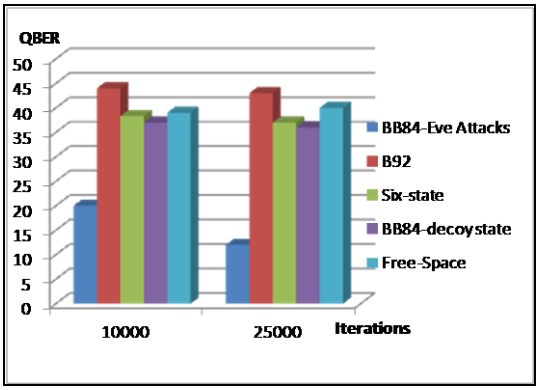


Figure 8. Practical Channel & Ideal Receiver

Fig. 9 shows the result of the protocol with the setting of eavesdropping technique and noise channel. All the protocol suffers huge reduction in QBER rate. The QBER rate reaches lesser than 25%. If the experimental detectors setting and faint-laser included, then the result almost equals to the experimental QKD.

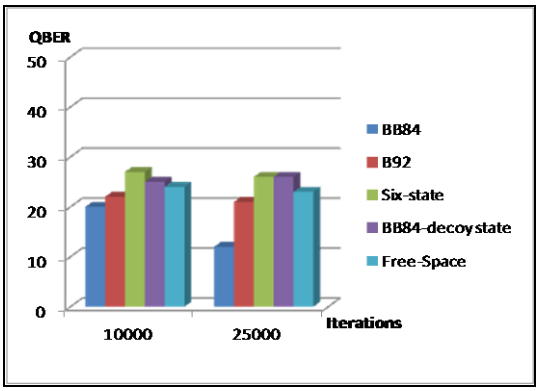


Figure 9. Practical Chanel with Eve Attack & Ideal Receiver

V. CONCLUSION

We have presented a simulation library and environment to simulate and evaluate QKD protocols in OptiSystem. The development phase and execution phase are complied with real QKD experiments. Moreover, proposed simulation library satisfies highly on some quality requirements. However, lack of detector implementation and assumption of the single photon reduces the accuracy of the results. The analyzed results show nearly equivalent with experimental results. Other encoding schemes and entanglement based QKD are our future concerns. This proposed simulation package can assist the researchers to test their models prior to real implementation. Further, the graphical oriented, easy to develop and reliable results are the attracting features for education purpose and new researchers.

REFERENCES

[1] [1] C.H. Bennett, and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," IEEE Internatioonal Conference Computer Systems and Signal Processing, Banglore, page 175, Bangalore, 1984.

[2] [2] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states," Physical Review Letters, vol. 68, no. 21, 1992, pp. 3121-3124.

[3] [3] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Physical Review Letters, vol. 92, no. 5, 2004, pp. 57901.

[4] [4] D. Bruß, "Optimal eavesdropping in quantum cryptography with six states," Physical Review Letters, vol. 81, no. 14, 1998, pp. 3018-3021.

[5] [5] H. Bechmann-Pasquinucci, and N. Gisin, "Incoherent and coherent eavesdropping in the 6-state protocol of quantum cryptography," Arxiv preprint quant-ph/9807041, 1998.

[6] [6] H.K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Physical review letters, vol. 94, no. 23, 2005, pp. 230504.

[7] [7] W. Buttler, R. Hughes, P. Kwiat, S. Lamoreaux, G. Luther, G. Morgan, J. Nordholt, C. Peterson, and C. Simmons, "Practical free-space quantum key distribution over 1 km," Arxiv preprint quant-ph/9805071, 1998.

[8] [8] R.J. Hughes, J.E. Nordholt, D. Derkacs, and C.G. Peterson, "Practical free-space quantum key distribution over 10 km in daylight and at night," New journal of physics, vol. 4, 2002, pp. 43.

[9] [9] C. Kurtsiefer, P. Zarda, M. Halder, P. Gorman, P. Tapster, J. Rarity, and H. Weinfurter, "Long distance free-space quantum cryptography," New journal of physics, vol. 4, 2002, pp. 43.41-43.14.

[10] [10] An Efficient Modeling and Simulation of Quantum Key Distribution Protocols Using OptiSystem™, 2012 IEEE Symposium on Industrial Electronics & Applications (ISIEA 2012) in Press.

[11] [11] Z.D. Walton, A.V. Sergienko, B.E.A. Saleh, and M.C. Teich, "Noise-Immune Quantum Key Distribution," Quantum communications and cryptography, 2006, pp. 211.

[12] [12] http://www.optiwave.com/.

[13] [13] http://csrc.nist.gov/groups/ST/toolkit/rng/index.html

[14] [14] S. Félix, N. Gisin, A. Stefanov, and H. Zbinden, "Faint laser quantum key distribution: Eavesdropping exploiting multiphoton pulses," Journal of Modern Optics, vol. 48, no. 13, 2001, pp. 2009-2021.

[15] [15] J. Anders, H.K. Ng, B.G. Englert, and S.Y. Looi, "The Singapore Protocol: Incoherent Eavesdropping Attacks," Arxiv preprint quant-ph/0505069, 2005.

[16] [16] W.H. Kye, and M.S. Kim, "Security against the Invisible Photon Attack for the Quantum Key Distribution with Blind Polarization Bases," Arxiv preprint quant-ph/0508028, 2005.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security

IJCSIS 2013
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500
http://sites.google.com/site/ijcsis/